

GUIDE FOR CREATING INTERNAL WRITTEN PROCEDURES REGARDING CRIMINAL HISTORY RECORD INFORMATION (CHRI) FOR A NON-CRIMINAL JUSTICE AGENCY (NCJA)

You will want to put enough information into your Internal Written Procedure regarding the process of CHRI & Fingerprinting so that your authorized personnel know where to start and what to do. Everyone that has access to CHRI should know the basics on how to submit fingerprints from start to finish & the proper use, handling & storage of CHRI.

Fingerprint Submissions & Process

- ☐ **What is your Agency account Number?**
- ☐ **What is your Agency ORI?**

Is the applicant being told where to go to get fingerprinted?

- ☐ If so, are prints given back to the applicant or are they transmitted to DPS-RCCD
- ☐ Will your agency be using Live Scan or Manual Fingerprint cards for fingerprint submissions?
- ☐ How does your agency ensure Manual Fingerprint Cards are not tampered with from the fingerprint site, until the applicant gives the cards back?

Is the purpose for fingerprinting the applicant appropriately written on the fingerprint card or reason fingerprinted on the fingerprint request form?

- ☐ Is authority being correctly recorded in the Reason Fingerprinted box?
- ☐ Has the applicant been provided with the appropriate information that the fingerprinting agency requires to transmit fingerprints? (i.e. the Fingerprint Request Form)
- ☐ Has the applicant been told what information is needed to properly fill out the fingerprint card?
- ☐ Has the applicant been properly identified?

What is the agency's process?

- ☐ Where in the agency's application/on boarding process is the applicant/licensee filling out the fingerprint background waiver?
- ☐ Are all applicants signing the fingerprint background waiver(s)?
- ☐ Are the applicants given any other waivers to sign?
 - i.e. NCPA/VCA VECHS Waiver (if applicable to authority)
- ☐ Is the agency keeping the fingerprint background waiver for an audit cycle? (3 years)
- ☐ Is the agency keeping supporting documentation of the applicant for an audit cycle? (3 years)

Use- Purpose for which CHRI is requested.

What is the authorization for the agency to submit fingerprints?

- ☐ What is the specific authority the agency uses to submit fingerprints?
 - i.e. What Nevada Revised Statute or Public Law does your agency run fingerprints under?

For what specific purpose(s) does the agency submit fingerprints?

- ☐ Are agency personnel aware of the agency's specific purpose(s)?
 - i.e. Employment, Volunteer, Licensing.
- ☐ Is each purpose consistent with the agency's authorization?
- ☐ Does your agency apply a list of disqualifiers on the record received?

For cities and counties: **NOT APPLICABLE TO YOU IF YOU ARE NOT A CITY OR COUNTY**

- ☐ Has your authorizing ordinance been repealed and replaced? If so, has the authorization been resubmitted to DPS for approval?
- ☐ Has the authorizing city code been changed/moved within the code? If so, has the authorization been resubmitted to DPS for approval?

Process & Handling of CHRI

Does the agency have written processes regarding the proper handling of CHRI from receiving point through destruction?

- ☐ Where and by whom is CHRI received into the agency?
 - Who opens/reviews the information?
 - Who has access to the NCCIS FlexCheck portal?
 - Who has access to the mail?
 - Where does it go from the receiving point?
 - Does the agency know how to properly read the CHRI results, to include warrants?
 - Where does primary review/handling take place?
 - Is the CHRI retained?
 - Who discusses CHRI with the applicant?
 - If discussed, what is put in place to make note of dissemination?
- ☐ Does the agency have policies regarding communication about CHRI?
 - Are there guidelines for communication among Authorized Personnel?
 - Are there guidelines for communication with the applicant?
 - Is the applicant given time to challenge their record if they are not chosen for employment?
 - Does your agency have a process for the applicant to appeal the decision if they are not selected for employment?
- ☐ Does the agency secondarily disseminate information?
 - What is the reason for the dissemination?
 - Does the agency have policies regarding the circumstances under which the CHRI is disseminated?
 - Does the agency keep a dissemination log with the required information?
 - Does the agency have a method for verifying the authenticity of the recipient of the CHRI?
- ☐ Are personnel aware that CHRI is not public record?
- ☐ Is CHRI stored separately from public records?

Is the agency advising the applicant of the review and challenge process?

- ☐ Does the agency notify the applicant how to obtain a copy of the FBI criminal history record?
- ☐ Does the agency have a documented procedure for any appeals process available to the applicant?
- ☐ Is the applicant given a reasonable period of time to appeal the decision?
- ☐ Does the agency have documented process for what constitutes a reasonable period of time?
- ☐ What is the agency's process to advise all applicants of the ability to review and challenge the criminal history record?
- ☐ Does the agency advise applicants to contact DPS for a Nevada record review and the FBI for a federal record review?

Outsourcing- Defined

- ☐ Does your agency Outsource?
 - Has your agency gotten approval from DPS RCCD to outsource?
 - What type of outsourcing does your agency participate in?
 - Are the employees of the outsourced agency properly trained? Is there documentation of their training?
 - Does your agency conduct audits with the outsourced agency?
 - How often are they audited?
- ☐ Outsourcing incorporates a third-party contractor that performs noncriminal justice administrative functions such as
 - Archival & Off-site storage, destruction, and or shredding of CHRI & fingerprints
 - Making fitness determinations & recommendations
 - Obtaining missing dispositions

Access- Who is authorized and how do you restrict access to only Authorized Personnel

Is the Authorized Personnel List current?

- ☐ Has the agency had personnel turnover affecting the list? Have qualified new hires been added to the list?
- ☐ Is everyone with a “need to know access” on the list?
- ☐ Do all authorized personnel have an NCCIS FlexCheck user account?
- ☐ Who are the authorized recipients on the account? They should be listed as a point of contact (POC) on the account. (Note: They will be the liaison between DPS and your agency.)
- ☐ Is an employee locked out of NCCIS IAM upon termination?
- ☐ How long after termination of an employee are they locked out of the NCCIS system?

Storage- How is the agency storing CHRI & other documents for upcoming audits

- ☐ Is the agency keeping the fingerprint background waiver for an audit cycle? (3 years)
- ☐ Is the agency keeping supporting documentation of the applicant for an audit cycle? (3 years)
- ☐ Where/how does the agency store CHRI prior to its destruction?
 - How is the CHRI downloaded off of the NCCIS FlexCheck portal?
 - Is the storage secure? (Locked room, locked cabinet, secure perimeter?)
 - Who has access to the room or secured area?
 - Does the agency have rules regarding not leaving CHRI unattended when it is not physically secured?
- ☐ How long does the agency retain CHRI?
 - What is the purpose/authorization for retention?
 - Does the agency have policies/procedures regarding retention rules?
 - Is the CHRI stored electronically?
 - If yes, do you have a technical audit established with DPS’s Information Security Officer?
 - Does the agency destroy CHRI when its purpose has been fulfilled and regulatory guidelines have been satisfied?

Destruction- How does the agency destroy CHRI & by who

- ☐ Who is responsible for the destruction of CHRI?
- ☐ How is it destroyed? Shredded? Burned?
- ☐ Is it destroyed on site or offsite?

Training- Agency Training Procedures

- ☐ Are all authorized personnel enrolled into CJIS Online?
- ☐ Has the POC and authorized personnel taken the Non-Criminal Justice Training and the Security and Privacy training and the Non Criminal Justice Agency training?
- ☐ Has CJIS Security and Privacy Training been completed by all authorized personnel?
- ☐ How often is recertification required for all authorized personnel and POC? (Annually)
- ☐ Are training certificates retained on file by the active authorized personnel for an audit cycle? (3 years).
- ☐ Is POC aware of their responsibilities? If yes, what are they?
- ☐ If your agency outsources, are those employees that have access to CHRI properly trained?

General Administration

Is the user agreement current?

- ☐ Has the responsible signer left the agency?
- ☐ Has the name of the agency changed?
- ☐ Has there been any change in the access authorization?
- ☐ Does the authorization cited in the user agreement reflect the current version of the authorization?

Is the current agency information on file at DPS?

- ☐ Is the Primary point of contact information current?
- ☐ Has the agency name, phone number, or address changed?
(Note: any changes to your account, DPS must be notified within ten days of the change.)
- ☐ Is the primary point of contact enrolled into IAM & Flexcheck?
- ☐ Is the primary point of contact enrolled into the Listerv that DPS uses to send out important notifications?
- ☐ Is the agency aware of how often NCU audits their agency?
- ☐ Is the agency enrolled into CJIS Audit Tool?

Questions/Concerns regarding Training or Audits please reach out to the below contacts

- ☐ Supervisor for Civil Audit Team: Casondra Ashbaugh (775) 684- 6243
- ☐ Civil Trainer: Meighan Quinn (775) 684-6260
- ☐ Civil Auditor: Holly Polson (775) 684-0924
- ☐ Civil Auditor: Vacant (775) 684-6246
- ☐ Civil Auditor: Samantha Snyder (775) 684-6284
- ☐ Supervisor for NCJIS Service Desk Team: Tiffany Alexander (775) 684- 6262 x 8
civilauditors@dps.state.nv.us or NCJISHELP@dps.state.nv.us

This document should be written on your agency's own letterhead. Please replace items in **BLUE** with information specific to your agency. Provide additional information where needed.

AGENCY NAME

Noncriminal Justice Agency Authorized Recipient

Internal Written Procedures

FINGERPRINT SUBMISSIONS:

Agency Account Number: _____

Agency ORI: _____

(Please see Internal Written Procedures Guide for further information)

USE/PURPOSE:

Criminal History Record Information (CHRI) is used by **AGENCY NAME** for **EMPLOYMENT AND/OR VOLUNTEER AND/OR LICENSING** purposes. **AGENCY NAME** submits fingerprints to the NV Department of Public Safety under the _____ authority. CHRI obtained under such authority may be used solely for the purpose for which the record was requested.

(Please see Internal Written Procedures Guide for further information)

PROCESS/HANDLING

Explain your agencies' application process for either employment or licensing and where in the process is the applicant given the Fingerprint Background Waiver to sign and date.

Prior to fingerprinting, applicants complete a signed and dated Fingerprint Background Waiver and NCPA/VCA Notice to Applicant Waiver (if applicable). These waivers are maintained on file by **AGENCY NAME** for one full audit cycle (3 years).

AGENCY NAME submits fingerprints for processing **MANUALLY / ELECTRONICALLY**. The applicant is provided a Fingerprint Request Form and sent to **FINGERPRINTING SITE (WHAT FINGERPRINTING NAME & LOCATION WILL YOUR AGENCY BE USING?)**

Once processed, Criminal History Record Information (CHRI) is accessible to **AGENCY NAME & ADDRESS** via the FlexCheck portal. CHRI is only reviewed by authorized personnel to make an eligibility determination.

AGENCY NAME (WILL OR WILL NOT) disseminate the CHRI to the subject of record if requested and will maintain a secondary dissemination log. **Does your agency plan on disseminating the Criminal History Records information to the subject of record?**

AGENCY NAME Challenge and hearing process for applicants is as follows: **Does your agency have a challenging process if an applicant wants to challenge the decision made by your agency if they are not hired for employment or licensing? If your agency has no internal process for challenge and appeals process, the applicant must still be given an appropriate amount of time to challenge their record. (Please see Internal Written Procedures Guide for further information)**

OUTSOURCING (ONLY APPLICABLE IF YOUR AGENCY OUTSOURCES)

Outsourcing incorporates a third-party contractor that performs noncriminal justice administrative functions such as

- Archival & Off-site storage, destruction, and or shredding of CHRI & fingerprints.
- Making fitness determinations & recommendations
- Obtaining missing dispositions

Agencies are only allowed to outsource if they have received approval from DPS- please reach out to your auditor if your agency is interested in outsourcing and the proper documents will be provided.

(Please see Internal Written Procedures Guide for further information)

STORAGE/DESTRUCTION

Hard copy/Electronic Copy of Criminal History Record Information (CHRI) received from the Nevada Department of Public Safety IS/IS NOT retained. (If retained; what records & supporting documents are kept & for how long?) **An example of proper storage/destruction:** Hard copies of these records are maintained in a locked, secured records environment accessible only by trained authorized personnel. OR The electronic copies of these records are stored electronically and are encrypted/stored within physically secure locations and/or controlled areas with restricted access. If your agency digitally stores CHRI, a technical audit must be established with the Department of Public Safety Information Security Officer. A technical audit with the Department of Public Safety Information Security Officer has been established.

CHRI is stored LOCATION.

CHRI shall be maintained in a locked secured records environment until it is destroyed. CHRI is destroyed by or under the observation of authorized personnel by shredding or burning & location of destruction.

(Please see Internal Written Procedures Guide for further information)

ACCESS

Only staff members listed on the Authorized Personnel List have access to Criminal History Record Information (CHRI). Training Documentation for every annual training certificate of completion is kept on file for all active authorized personnel for an audit cycle. (every training, for every year on all authorized staff will be kept on file for an audit cycle of 3 years)

FlexCheck is the portal used to access the fingerprint based CHRI. The proper role is assigned to the agency's main point of contact. If there are other authorized personnel that need direct access to CHRI through FlexCheck, it is the POC's responsibility to enroll them with their proper role. There are three roles, Agency Admin, Fiscal User and FlexCheck user.

Does the main point of contact have the proper role assigned in FlexCheck? Does HR or their fiscal employees need access to FlexCheck and have the proper roles assigned?
Does the main point of contact know what their responsibilities are? Please list them.

(Please see Internal Written Procedures Guide for further information)

TRAINING

The main point of contact for the agency shall be enrolled as the administrator for their agency's CJIS Online account. All authorized personnel shall be trained in Security and Privacy Training (CJIS Online) and internal agency training on the agency's security and handling processes prior to being allowed access to criminal justice and/or criminal history record information. As well as the Noncriminal Justice Agency Training (NCJA) in CJIS Online. The Security and Privacy training and NCJA training for all personnel shall be completed annually.

[\(Please see Internal Written Procedures Guide for further information\)](#)

GENERAL ADMINISTRATION

- Is the User Agreement current?
- Is all contact information updated within 10 days of the change -Does DPS know who the main point of contact is for your account?
- Does your agency have a copy of the CJIS Administrative Policy & are you aware of what it says?
- Do you know who your Civil Audit team is & how to contact them with questions?



Next Generation Identification Audit

Noncriminal Justice Access to Criminal History Record Information

Policy Reference Guide



Telephone – 304–625–3020
E-mail – <NGIAudit@leo.gov>

Table of Contents

Criminal History Record Information.....	1
Use of CHRI.....	2
Fingerprint-based	
Coordination and Approval	
Authorized Requests	
Implementation	
Re-use	
Name-based	
Coordination and Approval	
Authorized Requests	
Implementation	
Re-use	
Dissemination of CHRI.....	5
Authorized Recipients	
Receiving Departments	
Related Agencies	
Single Need/Purpose	
Multiple Needs/Purposes	
Other Authorized Entities	
Jurisdictional Control	
Public Access	
Additional Considerations	
General	
Notifications	
Subject of the Record	
Residual Access	
Purpose for Disclosure of CHRI.....	11
Reason Fingerprinted Field	
Interstate Identification Index Purpose Codes	
Reason for Request	
Agency Identifiers for Receipt of CHRI	
Independent Application, Fingerprinting, and Adjudication Processes	
Documentation of Reason for Request	
Applicant Notification	12
FBI Privacy Act Statement	
FBI Record Access and Amendment	
Additional Considerations	
Noncriminal Justice Agency Audits	17
User Fee	17
Criminal Justice (No-fee)	
Volunteer (Reduced-fee)	
Abbreviations and Acronyms	19

Criminal History Record Information

The Compact, at Title 34, U.S.C., Section 40316, Article I, includes the same statutory definition of CHRI as that established at Title 28, CFR, Section 20.3: information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, and release; the term does not include identification information such as fingerprint records if such information does not indicate the individual's involvement with the criminal justice system. In addition, the *CJIS Security Policy* defines CHRI as a subset of Criminal Justice Information consisting of any notations or other written or electronic evidence of an arrest, detention, complaint, indictment, information, or other formal criminal charge relating to an identifiable person that includes identifying information regarding the individual as well as the disposition of any charges.

Information is considered CHRI if it is transferred or reproduced directly from CHRI received as a result of a national FBI check and associated with the subject of the record. This includes information such as conviction/disposition data as well as identifiers used to index records regardless of format. Examples of formal and informal products or verbalizations include: correspondence such as letters and e-mails; documents such as forms and hand-written notes; conversations either in person or by telephone; and data fields such as those stored in database tables or spreadsheets. However, information is not considered CHRI if it is obtained as a result of using CHRI received from a national FBI check as a lead to reach out to source record owners such as local courts or state criminal history record repositories. As a prerequisite, both the process used to obtain the source record information and the resulting source record information itself must not directly reference or be attributed to the national FBI check.

Information is considered CHRI if it confirms the existence or nonexistence of CHRI. This FBI policy is derived from and mirrors the general policy on dissemination found at Title 28, CFR, Section 20.21, directly relating to applicable state and local criminal history record information systems. This includes applicant status information, which is either directly attributed to or predominately based on a national FBI check, when no recognized authority or inherent need exists for the release of such information.

Use of CHRI

The requirements for the use of CHRI for noncriminal justice purposes are derived from various federal statutes, regulations, policies, and interpretations thereof, to include rules and procedures promulgated by the Compact Council. Primary references for these requirements include:

- Title 28, U.S.C., Section 534 (a)(4)
- Title 34, U.S.C., Section 40316, Article IV (c) and Article V (a) and (c)
- Title 28, CFR, Section 20.33
- Title 28, CFR, Section 50.12
- Title 28, CFR, Section 901
- *III/NFF Operational and Technical Manual*, Chapter 3
- CJIS Advisory Policy Board, *Concept for the Exchange of Criminal History Records for Noncriminal Justice Uses by Means of The III*, Section B
- Compact Council's Noncriminal Justice Online Policy Resources

The NGI audit assesses four categories of requirements associated with the use of CHRI for noncriminal justice purposes: (1) Coordination and Approval, (2) Authorized Requests, (3) Implementation, and (4) Re-use. While baseline requirements for both fingerprint-based and name-based use of CHRI for noncriminal justice purposes essentially parallel one another, the four categories of requirements are presented from both perspectives for clarity and reporting purposes.

Use of CHRI (Fingerprint-based)

Unless authorized pursuant to federal statutory authority or Compact Council regulations promulgated based upon federal statutory authority, noncriminal justice background checks of the III System must be supported by fingerprints or other approved forms of positive identification in order to determine that the subject of a record search is the same person as the subject of a criminal history record indexed in the III System. This requirement is memorialized in the Compact. The Compact Council has accepted two methods for determining positive identification for exchanging CHRI for noncriminal justice purposes, ten-rolled fingerprints and ten-flat fingerprints.

Coordination and Approval

Agencies must only leverage recognized/approved authorities for submission of noncriminal justice fingerprint-based requests for CHRI. Examples of such authorities include Public Law 92-544, the NCPA/VCA, the Adam Walsh Act, and the Serve America Act. Prior to implementation of any federal statutory authority, a state or federal agency must coordinate with the FBI to determine the requirements for submitting under the specific authority (e.g., system changes, issuance of an ORI, fingerprint submission procedures, use of specific reason fingerprinted, etc.), and when applicable, obtain formal approval prior to use. When applicable, agencies must also obtain updated approval from the FBI for any changes associated with a previously approved authority, such as Public Law 92-544 state statutes. In addition, agencies must notify the FBI which authority is the exclusive remedy when multiple approved authorities exist for a particular purpose (applicant type). This specific requirement currently applies when states must formally designate either an approved Public Law 92-544 state statute or the NCPA/VCA for providers of care to vulnerable populations if state law is not clear or silent on the NCPA/VCA.

Authorized Requests

Agencies must only submit noncriminal justice fingerprint-based requests for CHRI for purposes (applicant types) covered by the authority leveraged for the request. In addition, agencies must only submit requests for purposes that are known to exist at the time of submission. Agencies must not submit requests for a future anticipated need, even if the need is covered by an approved authority.

Implementation

Agencies must implement all applicable administrative and procedural provisions associated with the authority leveraged to submit noncriminal justice fingerprint-based requests for CHRI (e.g., signed applicant statements under NCPA/VCA and VECHS agency user agreements).

Re-use

Agencies must only use CHRI received as a result of noncriminal justice fingerprint-based requests for the specific purpose originally requested. Agencies must not subsequently re-use CHRI for unrelated needs, even if the new needs are covered by a recognized/approved authority. A purpose or need for use is a request for CHRI to adjudicate a specific application for a noncriminal justice purpose (e.g., license, position of employment, benefit, etc.) that is known at the time the request is made, pursuant to an approved statutory authority, and based on the positive identification via fingerprint submission of the applicant. The basic parameters for use consists of (chronologically): 1) authority for access, 2) application and fingerprint submission, 3) receipt of CHRI, 4) adjudication, and 5) closing or maintenance activities.

However, if a special set of circumstances exist that show an extremely close relation to the original purpose, CHRI that was made available for the original purpose could possibly be used again for the new purpose. Under this premise, the new purpose is so closely related to the original purpose that both are considered singular in nature. The primary factors when considering the circumstances that may potentially relate multiple purposes include: the statutory authority being used; the agency or agencies involved; the type of license/position of employment/benefit being applied for; and the application/adjudication process. This consideration is based on standing audit practices and legal interpretations of related agency as applied to the use of CHRI. It is important to note that this type of acceptable re-use is quite infrequent and very dependent upon the specific scenario involved. As such, it is highly recommended that re-use of this nature be closely coordinated with the FBI prior to implementation. For example, a person applies to be a substitute teacher with public School Board A. School Board A completes the fingerprint process and submits the fingerprints pursuant to an approved state statute that authorizes background checks for school employment purposes. Then one month later the individual also applies to be a substitute teacher with public School Board B. School Board B requests a copy of the CHRI from School Board A which provides it. In this case, since School Board A and School Board B are both covered by the same statute and using CHRI for a similar applicant type within a relatively short period of time, these can be considered to be for the same purpose. However, if the applicant had applied one month later for a liquor license from the ABC Board, School Board A would not be permitted to provide the CHRI to the ABC Board. Although the background checks are in a relatively short period of time of each other, the applicant types are significantly

different enough, and the ABC Board would not be covered by the same statutory authority as School Board A. In addition, CHRI may be re-used in limited circumstances under the NCPA/VCA VECHS program.

It is important to note that FBI CHRI is considered instantly outdated as new information may be added to the record or deleted at any time. Although re-use of CHRI in certain situations may be acceptable, agencies that accept the risk of using outdated CHRI must understand that the information is subject to change.

Use of CHRI (Name-Based)

Access to the III System using name-based queries and record request messages is not permitted for noncriminal justice purposes, unless authorized pursuant to federal statutory authority or Compact Council regulations promulgated based upon federal statutory authority.

Coordination and Approval

Agencies must only leverage recognized/approved authorities for submission of name-based noncriminal justice III System queries and record request messages. Examples of such authorities include the Compact Council's Fingerprint Submission Requirements Rule (Purpose Code X), the Housing Opportunity Extension Act (Purpose Code H), and the Security Clearance Information Act (Purpose Code S). When applicable, agencies must coordinate with the FBI to determine specific requirements for use of a particular authority and obtain formal approval prior to use (e.g., Purpose Code X). When applicable, agencies must also obtain updated approval from the FBI for any changes associated with a previously approved authority.

Authorized Requests

Agencies must only submit name-based noncriminal justice III System queries and record request messages for authorized purposes covered by the authority leveraged for the request (i.e., federal statutory authority or Compact Council regulations promulgated based upon federal statutory authority). In addition, agencies must only submit requests for purposes that are known to exist at the time of submission. Agencies must not submit requests for a future anticipated need, even if the need is covered by an approved authority.

Implementation

Agencies must implement applicable administrative/procedural provisions required by the authority leveraged to submit name-based III checks for noncriminal justice purposes (e.g., follow-up fingerprints for Purpose Code X and limits on direct access by public housing authorities for Purpose Code H).

Re-use

Agencies must only use CHRI received as a result of noncriminal justice name-based III System queries and record request messages for the specific purpose originally requested. Agencies must not subsequently re-use CHRI for unrelated needs, even if the new needs are covered by a recognized/approved authority. Congruent with requirements for CHRI received as a result of fingerprint-based requests, re-use of CHRI received via name-based III checks may be acceptable in limited circumstances.

Dissemination of CHRI

The requirements for the dissemination of CHRI for noncriminal justice purposes are derived from various federal statutes, regulations, policies, and interpretations thereof, to include rules and procedures promulgated by the Compact Council. Primary references for these requirements include:

- Title 28, U.S.C., Section 534 (a)(4)
- Title 34, U.S.C., Section 40316, Article IV (c)
- Title 28, CFR, Section 20.33
- Title 28, CFR, Section 50.12
- Title 28, CFR, Section 906
- *III/NFF Operational and Technical Manual*, Chapter 3
- Compact Council's Noncriminal Justice Online Policy Resources

The NGI audit assesses three categories of requirements for dissemination of CHRI for noncriminal justice purposes: (1) Authorized Recipients, (2) Jurisdictional Control, and (3) Public Access. These categories center on the baseline requirement for allowable dissemination to receiving departments, related agencies, and other authorized entities. It should be noted that while the requirements below are written primarily from a state perspective, they also apply to federal and federally-regulated agencies that request, receive, and use CHRI for noncriminal justice purposes.

Authorized Recipients (Receiving Departments and Related Agencies)

CHRI may only be disseminated to receiving departments and related agencies that are authorized relative to the federal statutory authority used to obtain CHRI. States must ensure that recipients fall within allowable parameters established by federal statutory authorities leveraged for national criminal history checks.

As with the use of CHRI, parameters for dissemination are derived from the specific federal statutory authority leveraged to obtain CHRI. CHRI may only be disseminated to entities that are authorized relative to the federal statutory authority used to submit a fingerprint check. For example:

- Dissemination is limited to officials of state and local governments for CHRI obtained pursuant to Public Law 92-544.
- Dissemination is limited to "authorized agencies" defined as a division or office of a state for CHRI obtained pursuant to the NCPA/VCA. However, dissemination of CHRI is extended to nongovernmental qualified entities if a VECHS program is implemented.
- Dissemination is limited to the following entities for CHRI obtained pursuant to the Adam Walsh Act: 1) child welfare agencies, which include states, local agencies, other public agencies, or any other private agencies under contract with a state or local agency responsible for licensing or approval of foster or adoptive parents; and 2) public or private elementary or secondary schools as well as state and local educational agencies.
- Dissemination is limited to governmental agencies for CHRI obtained pursuant to the Serve America Act.

It is important to recognize that state or local laws, ordinances, administrative rules, or procedures may not be more permissive regarding dissemination of CHRI relative to the federal

authority used to obtain CHRI. However, states may be more restrictive and establish additional limitations on dissemination.

Receiving Departments

States should designate primary authorized recipients responsible for accessing or receiving CHRI directly from the state repository for noncriminal justice purposes. These agencies typically have statutory authority or regulatory obligations associated with making fitness determinations and/or providing oversight of the employment or licensing processes for particular categories of applicants. States must ensure that primary receiving agencies fall within parameters established by the federal statutory authorities being leveraged for national criminal history checks. CHRI may only be disseminated to entities that are authorized relative to the federal statutory authority used to obtain CHRI.

Depending upon the specific procedures used by a state, there may be multiple primary agency types with access to CHRI for a particular type of national criminal history check. For example, while one state's procedures may only include disseminating CHRI directly to a Department of Education for background checks of teachers, another state's procedures may include dissemination of CHRI directly to each local county school board. Still another state's procedures may include simultaneously disseminating CHRI directly to both the Department of Education and a local county school board.

The term "agency" encompasses offices, departments, bureaus, and other subdivisions associated with a particular agency's organizational structure. Although baseline dissemination requirements for CHRI are centered at the department and agency levels, as a best business practice, states should limit access to the minimum necessary sub-offices and personnel within a department or agency that are actually required for a particular use. While authorized receiving agencies may exercise some level of discretion and freedom of maneuver to distribute CHRI within their organizational structure, they should be able to demonstrate a reasonable need for doing so. For example, a local county school board may be designated as an authorized recipient of CHRI for the purpose of conducting background checks for prospective teachers. CHRI is stored as part of an electronic personnel records management system accessible by all school board employees. Although the school board is an authorized recipient, it is in the agency's best interests to limit access to CHRI on the system to only the personnel within the human resources department responsible for making fitness determinations. This will limit the school board's exposure to the inherent risks associated with unauthorized dissemination of CHRI.

Many statutory authorities leveraged for national criminal history record checks limit dissemination to governmental agencies. Most governmental agencies are readily identified, such as those statutorily designated, funded, and organized as part of a state's executive, legislative, and judicial branches. However, governmental entities, such as commissions and boards that may be comprised of political appointees, elected officials, and/or officials from private industry, may also qualify as authorized recipients of CHRI. Examples could include school boards and lottery commissions.

Related Agencies

Two primary categories of related agency exist with respect to dissemination of CHRI. The categories are based on the use of CHRI for a single need versus multiple needs, and are derived from historical definitions of related agency doctrine as well as standing audit practices and legal interpretations.

- *Dissemination of CHRI to related agencies for a single need/purpose.* This type of dissemination of CHRI occurs when multiple agencies are involved in making a single fitness determination associated with an application for a specific authorized noncriminal justice purpose, such as a license, position of employment, or benefit. In many instances, this type of related agency is a secondary recipient of CHRI from a primary agency that receives CHRI directly from the state level. The intent is to allow some level of flexibility within the allowable parameters established by the federal statutory authority being leveraged for the national criminal history check. For example, with the state's consent, the Department of Education and local county school boards are both involved in adjudication of teacher employment applications. In addition, on an ad-hoc basis, some of these local county school boards make CHRI available to their local Sheriff's Office in order to answer questions regarding specific charges on criminal history records. Another example includes, with the state's consent, the Bureau of Professional Licensing and the Real Estate Commission are both involved in adjudication of real estate license applications.
- *Dissemination of CHRI to related agencies for multiple needs/purposes.* This type of dissemination of CHRI occurs when multiple agencies are involved in making fitness determinations for separate but related needs associated with multiple applications for specific authorized noncriminal justice purposes, such as a license, position of employment, or benefit. This type of dissemination directly correlates to the re-use of CHRI for related needs as described in the Compact Council's online policy resource, *Use of FBI CHRI for Noncriminal Justice Purposes*. For example, if established requirements are met, there are limited instances when CHRI may be disseminated between agencies pursuant to the Public Law 92-544 Article IV sharing initiative or the NCPA/VCA VECHS program. However, just as CHRI must not be re-used for subsequent unrelated needs by the original requestor/recipient, it is imperative to recognize that CHRI must also not be disseminated to another recipient for subsequent unrelated re-use. In addition, CHRI may not be disseminated to another recipient for future anticipated uses, regardless of whether or not the needs are formally related.

Just as with the primary receiving agency, any related secondary recipient must also be authorized relative to the federal statutory authority used to obtain CHRI. For example, agencies related for the purpose of adjudicating an employment application for child day care pursuant to Public Law 92-544 must be governmental. Note that even though a private employer, such as a day care center, may be perceived as having a commonality of purpose, CHRI may not be disseminated to them by the governmental agency. States should be able to demonstrate a reasonable need for which they have designated agencies as related for the purpose of adjudicating a particular type of applicant.

It is important to recognize the distinction between authorized recipients, related agencies, and contractors. A related agency is essentially a specially designated authorized recipient with an inherent authority to access CHRI, and therefore does not require formal implementation of the Compact Council's *Security and Management Control Outsourcing Standard for Non-Channelers*. However, a governmental or private contractor has no such inherent authority, and therefore does require formal outsourcing implementation. Authorized recipients may not leverage outsourcing to create an authority for the intended purpose of designating an entity as a related agency. For example, pursuant to Public Law 92-544, local county school boards are typically considered to be related to the Department of Education; however, private schools would not be considered related agencies, because they are nongovernmental. As such, the Department of Education could not implement outsourcing to designate a private school as a "contractor" to allow the private school access to CHRI for the purpose of making fitness determinations on the private school's applicants. As an alternative, the state could consider leveraging the Adam Walsh Act or the NCPA/VCA VECHS program, both of which authorize dissemination to nongovernmental entities, thus designating such entities as authorized recipients.

Other Authorized Entities

For NGI audit purposes, other authorized entities represent assessments of specific requirements not directly assessed or reported as part of the Authorized Recipients category.

Jurisdictional Control

Agencies outside of a state's jurisdiction cannot be designated as related agencies, even when a congruent related need appears to exist for the use of CHRI. The dissemination restriction primarily centers on each state's individual authority and obligation to administer access to CHRI. Each state has the authority to determine whether or not to conduct particular types of noncriminal justice background checks, and each state is responsible for establishing the mechanisms and procedures for those checks within its jurisdiction. In addition, each state possess limited authority to meet obligations for maintaining appropriate controls, such as user agreements and audits, outside of its jurisdiction, especially with respect to another state's governmental agencies. In conjunction with the more obvious jurisdictional concerns associated with one state's governmental agency leveraging another state's statutes under Public Law 92-544, similar jurisdictional concerns also exist with the use of other statutory authorities such as the Adam Walsh Act or the NCPA/VCA. Examples of unauthorized dissemination include:

- One state governmental agency sharing CHRI with another state's governmental agency for adoption purposes when the child and prospective parents reside in different states, even if both states have approved Public Law 92-544 state statutes.
- Criminal history sharing initiatives involving participation in national compacts, associations, or databases such as those for child placement or employment/licensing in the health care industry.

This dissemination restriction is not intended to limit a state from making CHRI available in very limited situations to certain nongovernmental entities outside of the state's geographical boundaries when such dissemination is specifically authorized and formal jurisdictional authority is established to maintain adequate controls. It is very important to recognize that in order for dissemination to occur beyond a state's geographical

boundaries, there must first be an approved statutory authority which allows nongovernmental entities access to CHRI within the state's geographical boundaries. There must also be a recognized authority and obligation to formally establish security controls over the nongovernmental entities. For example, it is acceptable for a state to leverage an out-of-state private contractor for record archiving and destruction, since access to CHRI by private contractors is authorized pursuant to Title 28, CFR, Section 906, and jurisdictional authority for controls such as audits would be formally established through implementation of the *Security and Management Control Outsourcing Standard for Non-Channelers*.

Public Access

CHRI must not be disseminated to the general public. This includes maintaining CHRI in formats that are accessible by the public or within records that are subject to release through public record requests. However, CHRI may be disclosed as part of the adjudication process during a hearing that is open to the public if the agency demonstrates: 1) the hearing is based on a formally established requirement; 2) the applicant is aware prior to the hearing that CHRI may be disclosed; 3) the applicant is not prohibited from being present at the hearing; and 4) CHRI is not disclosed during the hearing if the applicant withdraws from the application process. For example, a board or commission may be authorized to access CHRI, and as part of regularly scheduled meetings, applicant appeals are discussed as standard agenda items. Even when the specific conditions are met to allow disclosure during a public hearing, the most preferable method for introducing CHRI is to enter into a closed session which limits participation by the public at large. States and local agencies should be able to reasonably demonstrate how the prerequisite criteria are being met for audit purposes.

Additional Considerations

Although not formal categories of assessment, the following considerations are applied to the assessment of requirements for dissemination of CHRI.

General

States need to maintain visibility on the full spectrum of primary agencies to which they disseminate CHRI, as well as the specific purposes/authorities for which those primary agencies receive CHRI. This is especially significant given the requirements for states to execute agency user agreements and establish formal noncriminal justice audit programs in accordance with the *CJIS Security Policy*.

Dissemination of CHRI is broader in concept than the simple act of physically or electronically sending CHRI to a recipient. The concept of dissemination also applies to making CHRI available to recipients through physical or electronic access. The overarching requirements associated with dissemination of CHRI apply regardless of whether CHRI is "pushed" to recipients or "pulled" by recipients since the end result is the same.

Notifications

The definition of CHRI includes information that confirms the existence or nonexistence of CHRI. This includes applicant status information, which is either directly attributed to or predominately based on a national FBI check, when no authority or inherent need

exists for the release of such information. However, if an inherent need does exist to advise a particular entity not otherwise authorized relevant to the federal statutory authority being leveraged for the national criminal history check, then it is acceptable to notify the entity of the outcome of applicant fitness determinations. Entities to which an applicant is seeking employment or licensing may receive status notifications which indicate the positive or negative outcome of fitness determinations. For example, a private day care center is not an authorized recipient of CHRI received pursuant to Public Law 92-544, but may be eligible to receive a status notification regarding an applicant who is seeking employment at the day care center (this assumes of course the approved state statute covers the employment type). States should be able to demonstrate the inherent need for which a particular entity is designated to receive status notifications. Status notifications must not contain CHRI to include confirming the existence or non-existence of CHRI. Generic “pass/fail” language must be used to the greatest extent possible, with the understanding that a reasonable balance must exist between the need to notify a potential employer and not indirectly confirming the existence or non-existence of CHRI. In addition, notification language should not directly reference that a national FBI check was conducted.

Subject of the Record.

Agencies may disseminate fingerprint-based CHRI obtained for noncriminal justice purposes to the subject of the record. It is important to note that agencies are under no direct obligation to provide CHRI to the subject, and dissemination of CHRI by local agencies to the subject may be limited at the state’s discretion. As a best business practice, agencies that disseminate CHRI to the subject of the record should verify the subject’s identity prior to dissemination and document each occurrence. Also, in order to limit potential risks associated with a subject’s subsequent use of a criminal history record, agencies may wish to consider marking the record in some manner to distinguish it as not an original copy.

CHRI may not be disseminated to spouses or other household or family members, even at the subject’s request. Further, CHRI may not be disseminated to other parties such as potential employers on behalf of the subject. However, although the preference is to disseminate directly to the subject of the record, a subject may request that their record be accessed by an attorney acting on the subject’s behalf. This scenario could potentially be encountered when an applicant challenges the outcome of an agency’s fitness determination as part of a formal appeal process.

Residual Access

Other authorized entities also include agencies which require residual access based on oversight authority and responsibility, such as the review of case files by an inspector general’s office or regulatory auditors from outside the receiving organization. Such access should be limited to only the minimum level necessary to accomplish oversight responsibilities, and controls should be established to reasonably prevent unauthorized disclosure of CHRI.

In limited circumstances, government agencies may also be related for the purpose of simply serving as a pass-through for fingerprints and receipt of CHRI. This typically occurs in situations when a criminal justice agency, such as a police department,

performs this specific function on behalf of an authorized recipient. The premise is that “access” to CHRI (view or make use of) is limited to such an extent to essentially consider it negligible for the purposes of formally categorizing it as access.

Purpose for Disclosure of CHRI

The Privacy Act of 1974 requires that the FBI’s CJIS Division keep an accurate accounting of the purpose of each disclosure of a criminal history record and the recipient of that record. (Title 5, U.S.C., Section 552a (c)(1)(A); *III/NFF Operational and Technical Manual*, Chapter 3, Section 2.1)

The NGI audit assesses three categories of requirements for the purpose for disclosure of CHRI: (1) Reason Fingerprinted Field, (2) III Purpose Codes, and (3) Reason for Request.

Reason Fingerprinted Field

All fingerprint-based applicant submissions must include in the reason fingerprinted field an accurate representation of the purpose and/or authority for which the CHRI is to be used.

III Purpose Codes

All name-based III inquiry and record request messages must include the correct purpose code for which the CHRI is to be used.

Reason for Request

All users are required to provide the reason for all name-based and fingerprint-based III transactions upon request by CJIS systems managers, administrators, and representatives. While the purpose code and reason fingerprinted field provide some lead information, they only provide a minimal audit trail. Requiring the specific reason for all III inquiries assists the FBI in ensuring III transactions are conducted for authorized purposes and purpose codes and RFPs are being correctly used. There is also an obligation to ensure requests for CHRI are being conducted for only authorized purposes prior to the submission of the request to the FBI. Submitting entities (e.g., state repositories) are ultimately responsible for ensuring these requirements are met throughout their applicable jurisdictions and should develop the policies, procedures, training, and controls necessary to ensure compliance. While submitting entities should be in a position to indirectly provide or otherwise facilitate providing specific reasons for requests for CHRI during FBI audits, typically local agencies and/or organizational subcomponents that receive and directly use CHRI to adjudicate applications are in the best position to provide specific validating information regarding individual applicants.

Agency identifiers for receipt of CHRI

The inability of an agency to provide a specific reason may be the indirect result of other compliance issues. If an agency receives CHRI for an individual that it has no knowledge of, then there may actually be a dissemination issue. For example, if a state uses a livescan vendor who makes an inaccurate selection of an agency’s Originating Agency Identifier (ORI) or other similar identifier, then the state may send the results to the wrong agency. Unlike the agency that is legitimately waiting for the CHRI, the receiving agency has no knowledge of the applicant and is not able to provide a reason for the submission when asked to do so. As a best business practice, when an agency receives CHRI on an individual that is unknown to the agency, it should inform the state

repository. This practice allows the state repository the opportunity to find out what went wrong with the submission and to ensure that the correct agency is not waiting any longer than necessary for the results of the submission. Submitting entities should also establish effective policies, procedures, and other controls necessary to minimize the risk of inaccuracies with fingerprint submissions that result in the wrong agency receiving CHRI.

Independent application, fingerprinting, and adjudication processes

In a traditional process model, a single agency might be responsible for receiving an individual's application, fingerprinting the applicant, and adjudicating the results of the background check. However, variations on this model have been implemented by agencies, whereby processes associated with receiving an application, obtaining fingerprints, and adjudicating results are independent or "split" from one another and/or performed by a separate entity. These variations may result in applicants being fingerprinted prior to submitting an application. The receipt of fingerprints prior to the application may cause an agency's inability to reasonably assure that the CHRI was for a legitimate purposes and/or the agency may have no knowledge of the applicant. Separate application, fingerprinting, and adjudication processes do not necessarily cause a compliance issue, but oversight agencies must provide sufficient management control to ensure agencies within their jurisdictions that implement such processes have adequate visibility and controls in place to reasonably reduce the risk of unauthorized requests for CHRI and to be able to provide a specific reason for the CHRI request.

Documentation of reason for request

Although agencies must be able to provide CJIS Systems managers, administrators, and representatives some level of specificity about the requests for CHRI in order for them to be "known," there is no direct requirement for an agency to maintain "case files" or other documents in order to support requests for CHRI. In order to meet the requirements for providing a specific reason for requests for CHRI, agencies must have a reasonable level of knowledge of the subject and the specific reason for requesting CHRI for that subject and be able to provide sufficient supporting information, regardless of format. While this is typically accomplished by providing a copy of an application corresponding to a request for CHRI, there are other means by which agencies are able to meet this requirement. A few examples of items that may be used to provide supporting information include: information contained in a personnel database or other information system; copies of online registrations; e-mails showing the purpose or the applicant's position; and supporting statements from applicable officials.

Applicant Notification

Authorized governmental and non-governmental agencies/officials that conduct a national fingerprint-based criminal history record check on an applicant for a noncriminal justice purpose (such as employment or a license, immigration or naturalization matter, security clearance, or adoption) are obligated to ensure the applicant is provided certain notices and other information and that the results of the check are handled in a manner that protects the applicant's privacy. All notices must be provided in writing. These obligations are pursuant to the Privacy Act of 1974, Title 5, U.S.C., Section 552a, and Title 28, CFR, Section 50.12, among other authorities. Primary references for these requirements include:

-
- Title 5, U.S.C., Section 552a (e)(3)
 - Title 28, CFR, Section 50.12
 - Compact Council Meeting, November 2019, Topic 4, Privacy Notice Fundamentals
 - Compact Council Brochure, Agency Privacy Requirements for Noncriminal Justice Applicants

The NGI audit assesses two categories of requirements for applicant notification: (1) FBI Privacy Act Statement and (2) FBI Record Access and Amendment.

FBI Privacy Act Statement

The Privacy Act of 1974 (Title 5, U.S.C., Section 552a) was enacted to balance the government's need to maintain information about individuals with the right of individuals to be protected from unwarranted invasions of privacy. The Privacy Act regulates the government's collection, maintenance, use, and disclosure of records about individuals. It applies to all federal agencies, including the FBI, and it applies to all systems of records maintained by those agencies, including the NGI system.

Certain parts of the Privacy Act are especially relevant to the NGI system, the National Crime Prevention and Privacy Compact Council (Council), and noncriminal justice background checks. Subsection (e)(3) of the Privacy Act provides the basis for the notice requirement when noncriminal justice fingerprints are collected for submission to the NGI system. The text of (e)(3) is as follows:

(e) Each agency that maintains a system of records shall-
(3) inform each individual whom it asks to supply information, on the form which it uses to collect the information or on a separate form that can be retained by the individual-
(A) the authority (whether granted by statute, or by executive order of the President) which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary;
(B) the principal purpose or purposes for which the information is intended to be used;
(C) the routine uses which may be made of the information, as published pursuant to paragraph (4)(D) of this subsection; and
(D) the effects on him, if any, of not providing all or any part of the requested information.

In order to comply with this section of the Privacy Act, the FBI requires that agencies must use the Privacy Act statement presented to, and approved by, the Council in 2013. This statement has been approved by the Office of Management and Budget (OMB) and is printed on the FD-258 fingerprint cards. This notice includes all of the required information, such as the authority, the principle purpose, and the routine uses. The Privacy Act statement is as follows:

Authority: The FBI's acquisition, preservation, and exchange of fingerprints and associated information is generally authorized under 28 U.S.C. 534. Depending on the nature of your application, supplemental authorities include Federal statutes, State statutes pursuant to Pub. L. 92-544, Presidential Executive Orders, and federal regulations. Providing your fingerprints and associated information is voluntary; however, failure to do so may affect completion or approval of your application.

Principal Purpose: Certain determinations, such as employment, licensing, and security clearances, may be predicated on fingerprint-based background checks. Your fingerprints and associated information/biometrics may be provided to the employing, investigating, or otherwise responsible agency, and/or the FBI for the purpose of comparing your fingerprints to other fingerprints in the FBI's Next Generation Identification (NGI) system or its successor systems (including civil, criminal, and latent fingerprint repositories) or other available records of the employing, investigating, or otherwise responsible agency. The FBI may retain your fingerprints and associated information/biometrics in NGI after the completion of this application and, while retained, your fingerprints may continue to be compared against other fingerprints submitted to or retained by NGI.

Routine Uses: During the processing of this application and for as long thereafter as your fingerprints and associated information/biometrics are retained in NGI, your information may be disclosed pursuant to your consent, and may be disclosed without your consent as permitted by the Privacy Act of 1974 and all applicable Routine Uses as may be published at any time in the Federal Register, including the Routine Uses for the NGI system and the FBI's Blanket Routine Uses. Routine Uses include, but are not limited to, disclosures to: employing, governmental or authorized non-governmental agencies responsible for employment, contracting, licensing, security clearances, and other suitability determinations; local, state, tribal or federal law enforcement agencies; criminal justice agencies; and agencies responsible for national security or public safety.

The requirement for a Privacy Act statement for the submission of noncriminal justice fingerprints is not new; however, it has become of greater importance due to the retention of such fingerprints in the NGI system and the Rap Back service. Because a right, benefit, or privilege is being granted based on the information collected, it is essential that the individual knows that the submission of his or her information is voluntary and knows what will happen with the information once it is submitted. The OMB, the agency that promulgates Privacy Act guidance and directives for the federal government, has opined that implicit in subsection (e)(3) is the idea of "informed consent", meaning that the individual should be provided with sufficient information to make an informed decision on whether to provide his information to the government.

Contributors of noncriminal justice fingerprints to the NGI system have inquired as to what constitutes a sufficient or adequate Privacy Act statement. The FBI requires that agencies use the current (i.e., 2013 or later) FBI Privacy Act statement, with additional language as necessary for state or federal agency purposes. If the agency does not use the exact language of the FBI Privacy Act statement, it must use language that is substantively similar to the FBI language. At a minimum, the language must address the submission of the fingerprints and associated information to the NGI system; the searching of the fingerprints against the civil, criminal, and latent repositories; and the continual comparison of the fingerprints to other fingerprints submitted to or retained by the NGI system.

Contributors of noncriminal justice fingerprints to the NGI system have requested clarification on best practices for providing the Privacy Act statement and how to effectively document those practices for auditing purposes. Since the Privacy Act was passed decades before our current electronic systems, it is important to comply with the statute but to also accommodate modern technology. In its Circular A-108, "Federal Agency Responsibilities for Review, Reporting, and

Publication Under the Privacy Act”, OMB stated that a Privacy Act statement is necessary “regardless of whether information is collected on a paper or electronic form, on a website, on a mobile application, over the telephone, or through some other medium”.

In past guidance to the Council, the FBI has advised that the Privacy Act statement must be provided in writing in order to comply with the statute, and that the notice may be provided in hard copy or in electronic format. For example, the notice may be provided on the hard-copy fingerprint card, on a form included with an application package, via an electronic notice on a live scan machine, or an electronic notice that must be viewed by the applicant before proceeding with the application. The agency must demonstrate that each individual received the Privacy Act statement. The FBI requires that the contributors have a verifiable process in place to ensure that all individuals have received the requisite Privacy Act statement. Simply providing a general notice, such as a poster on a wall or a notice on a website, will not be sufficient. The Privacy Act statement should be provided before or at the time of collection of the fingerprints in order to ensure informed consent and a copy should be provided to the individual if he or she requests it.

Contributors also have inquired as to how long they should maintain proof of having provided the Privacy Act statement to individuals. The FBI recommends that each agency follow its own record retention rules; however, the contributor will need to document the verifiable process to the CJIS Audit Unit when requested and for participation in Rap Back.

In the Spring of 2017, the “Noncriminal Justice Applicant’s Privacy Rights” and “Agency Requirements for Noncriminal Justice Applicants” brochures were modified to include an “acknowledgement” on the part of the individual receiving the Privacy Act statement. Although it would be a good practice for the individual to acknowledge receipt of the Privacy Act statement (e.g., the applicant checks a box on the live scan screen to confirm receipt of the notice), there is no requirement for the relevant agency to require or maintain such acknowledgements. Individual acknowledgments would certainly assist with documenting Privacy Act compliance and informed consent, but the statute requires that agencies provide the individual notice, not that the individual acknowledges receipt of that notice.

FBI Record Access and Amendment (28 CFR 50.12)

Subsection (d) of the Privacy Act contains the access and amendment provisions that require each federal agency that maintains a system of records to, upon request, permit the individual to gain access to his record or any information pertaining to him in the system and review the record and have a copy made. The Privacy Act also has procedures for an individual to request correction of his record if he believes it is not accurate, timely, relevant, or complete, and provides procedures if his request for correction is denied.

For access and amendment of criminal history records, the Department of Justice issued specific regulations found at 28 CFR 16.30-16.34 that require the individual to submit fingerprints, an application with certain biographic information, and a fee. If seeking a change, update, or correction to his or her record, the individual is generally directed to the agency that contributed the information to the FBI. This process is known as the “Departmental Order” process and has been briefed to the Council for many years. The “Departmental Order” process whereby an individual requests a copy of his or her criminal history record is simply the specific means by which the Privacy Act rights of access and amendment are implemented for criminal history records.

Another federal regulation, 28 CFR 50.12, requires that applicants receive notice that their fingerprints will be searched in the FBI's system and must be advised of their rights to seek a change, correction, or updating of their records pursuant to 28 CFR 16.34. The relevant text of 28 C.F.R. 50.12 is as follows:

Officials at the governmental institutions and other entities authorized to submit fingerprints and receive FBI identification records under this authority must notify the individuals fingerprinted that the fingerprints will be used to check the criminal history records of the FBI. The officials making the determination of suitability for licensing or employment shall provide the applicants the opportunity to complete, or challenge the accuracy of the information contained in the FBI identification record. These officials also must advise the applicants that procedures for obtaining a change, correction, or updating of an FBI identification record are set forth in 28 CFR 16.34. Officials making such determinations should not deny the license or employment based on information in the record until the applicant has been afforded a reasonable time to correct or complete the record, or has declined to do so. A statement incorporating these use-and-challenge requirements will be placed on all records disseminated under this program. This policy is intended to ensure that all relevant criminal record information is made available to provide for the public safety and, further, to protect the interests of the prospective employee/licensee who may be affected by the information or lack of information in an identification record.

If the applicant receives the current Privacy Act statement, the notice requirement of 28 CFR 50.12 regarding searching of the fingerprints to check the criminal history records of the FBI has been met. However, the agency also must be certain to provide written notice to the applicant regarding the procedures for accessing and amending his or her criminal history record. All applicants must be provided with such notice, regardless of whether the applicant, in fact, has any criminal history record information in NGI. The FBI recommends that agencies provide both the Privacy Act statement and the 28 CFR 50.12 notice at the same time and/or on the same document if possible, to ensure that the applicant receives all required notices.

In addition to the notice requirements of 28 CFR 50.12, the regulation requires that applicants must be afforded the opportunity to correct or complete criminal history records. This opportunity must be afforded whether the criminal history is actually used to disqualify the applicant or not. The CJIS Audit Unit ensures that agencies have a verifiable process in place to comply with this requirement.

28 CFR 50.12 states that applicants should not be denied employment or licensing based on information in the criminal history record until they have been afforded a reasonable time to correct or complete the record, or declined to do so. At Council meetings in 2011, the question of what constituted a "reasonable" time was discussed and the Council declined to define the term. The FBI does not consider this part of 28 CFR 50.12 to be a requirement because it states that officials "should" (rather than "must" or "shall") not deny employment or licensing. While it would be a best practice to have up-to-date and accurate criminal history information before making employment decisions, the FBI recognizes that many other considerations and limitations affect the hiring/licensing decisions.

Additional Considerations

The FBI recommends that agencies consult the “Noncriminal Justice Applicant’s Privacy Rights” and “Agency Requirements for Noncriminal Justice Applicants” brochures to ensure that all of the requirements pursuant to the Privacy Act and 28 CFR 50.12 are being met.

The FBI has no objection to officials providing a copy of the applicant’s FBI criminal history record to the applicant for review and possible challenge when the record was obtained based on positive fingerprint identification. If agency policy permits, this courtesy will save the applicant the time and additional FBI fee to obtain his/her record directly from the FBI by following the procedures found at 28 CFR 16.30 through 16.34. It will also allow the officials to make a more timely determination of the applicant’s suitability.

Each agency should establish and document the process/procedures it utilizes for how/when it gives the applicant the FBI Privacy Act statement, the 28 CFR 50.12 notice, and the opportunity to correct his/her record. Such documentation will assist State and/or FBI auditors during periodic compliance reviews on use of FBI criminal history records for noncriminal justice purposes.

Noncriminal Justice Agency Audits

Each CJIS Systems Agency, in coordination with the State Identification Bureau, shall establish a process to periodically audit all noncriminal justice agencies, with access to Criminal Justice Information, in order to ensure compliance with applicable statutes, regulations and policies. (*CJIS Security Policy, Section 5.11.2*)

User Fee

Agencies must ensure fingerprint-based requests for CHRI are properly submitted in order to ensure the appropriate application of user fees. Pursuant to Public Law 101-515, the FBI may establish and collect fees to process fingerprint identification records and name checks for noncriminal justice, non-law enforcement employment and licensing purposes.

The NGI audit assesses two categories of requirements for user fee: (1) Criminal Justice and (2) Volunteer.

Criminal Justice (No-fee)

Processing of fingerprint submissions for screening criminal justice agency employees or applicants for employment (sworn and non-sworn) are at no cost inasmuch as criminal justice employment is considered an administration of criminal justice function. (Title 28, CFR, Section 20.33 (a)(1))

In addition, processing of fingerprint submissions for screening those under contract with criminal justice agencies are at no cost under the following circumstances:

- The contractor is providing services for the administration of criminal justice.
- The contractor is performing services unrelated to the administration of criminal justice, but has unsupervised access to the facility (criminal justice agency site security).

However, fingerprint submissions for screening employees of contractors to whom the entire administration of criminal justice functions have been outsourced, such as private prisons and emergency dispatch centers, are subject to the user fee.

(*Criminal Justice Contract Employee Fingerprint Submission Summary Sheet*, September 2, 2003 and *CJIS Information Letter* 07-1, January 8, 2007)

It should be noted that the definition of “administration of criminal justice” appearing at Title 28, CFR, Section 20.3 (b) includes “Detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders.” However, it is recognized that there are other services which must be performed in support of these nine identified functions and hence, would also be considered an administration of criminal justice function. For example, personnel who transport, feed, provide medical (including psychiatric) care, teach and otherwise engage in the rehabilitative process also perform an administration of criminal justice function, although their functions are only implicitly contained within the regulatory definition.

Volunteer (Reduced-fee)

In the case of a background check conducted with fingerprints on a person who volunteers with a qualified entity, the fees collected by the FBI may not exceed eighteen dollars, or the actual cost, whichever is less. The Type of Search Requested field for applicable fingerprint submission transaction types must be set to a value of “V” to ensure proper processing.

(Title 34, U.S.C., Section 40102 (e); *Electronic Biometric Transmission Specification*, version 10.0.9, Appendix C, page C-40)

Abbreviation or Acronym	Term
Adam Walsh Act	Adam Walsh Child Protection and Safety Act
CFR	Code of Federal Regulations
CHRI	Criminal History Record Information
CJIS	Criminal Justice Information Services
Compact	National Crime Prevention and Privacy Compact
Serve America Act	Edward M. Kennedy Serve America Act
FBI	Federal Bureau of Investigation
III	Interstate Identification Index
NCPA/VCA	National Child Protection Act/Volunteers for Children Act
NFF	National Fingerprint File
NGI	Next Generation Identification
ORI	Originating Agency Identifier
U.S.C.	United States Code
VECHS	Volunteer and Employee Criminal History System
WAN	Wide Area Network

Next Generation Identification Audit Outline

Noncriminal Justice Access to Criminal History Record Information

This outline summarizes requirements for access to criminal history record information (CHRI) for noncriminal justice purposes assessed during Next Generation Identification audits conducted by the Federal Bureau of Investigation's (FBI) Criminal Justice Services (CJIS) Division, CJIS Audit Unit. The outline can be used as a checklist to conduct audits or to advise audit participants on what to expect during an audit. The outline serves as a supplement to the National Crime Prevention and Privacy Compact Council's (Council) *Audit Guide* and corresponds to requirements in the *Next Generation Identification Audit Noncriminal Justice Access to Criminal History Record Information Policy Reference Guide* and the Council's Noncriminal Justice Online Policy Resources.

1. Use of CHRI

a. Authorized Requests

- Fingerprint-based and name-based requests for CHRI must be submitted pursuant to an existing authority approved for use by the FBI.
- Subjects of a request for CHRI (i.e., applicant types) must be covered by the authority designated for use in requesting the CHRI.
- CHRI must not be requested for a future anticipated need (i.e., a need does not actually exist at the time the request is made).

b. Implementation

- Applicable administrative and procedural provisions associated with the authority designated for use in fingerprint-based and name-based requests for CHRI must be met.
- Examples of implementation requirements include:
 - Obtaining FBI approval of state statutes for use of Public Law 92-544.
 - Obtaining FBI approval for use of Sections 151 and 153 of the Adam Walsh Act.
 - Obtaining signed statements required by use of National Child Protection Act/Volunteers for Children Act (NCPA/VCA).
 - Obtaining signed waivers required by use of an NCPA/VCA VECHS program.
 - Obtaining FBI approval and use of a "Q" ending Originating Agency Identifier (ORI) for Purpose Code H name-checks required by use of the Housing Opportunity Program Extension (HOPE) Act.
 - Submitting follow-up fingerprints within 15 calendar days after conducting a Purpose Code X name-based check required by the Council's Fingerprint Submission Requirements rule and the Amended Florida Proposal.

c. Re-use

- CHRI received as a result of fingerprint-based and name-based requests must only be used for the specific purpose requested.
- CHRI received as a result of fingerprint-based and name-based requests may only be re-used for authorized purposes.
 - Coordination with the FBI is highly recommended prior to implementation of processes that include any re-use of CHRI.

Next Generation Identification Audit Outline
Noncriminal Justice Access to Criminal History Record Information

2. Dissemination of CHRI

a. Authorized Recipients

- CHRI received as a result of fingerprint-based and name-based requests must only be disseminated to authorized receiving departments and related agencies relative to the authority designated for use in requesting CHRI. Examples of dissemination requirements include:
 - CHRI obtained under Public Law 92-544, NCPA/VCA, and Serve America Act must only be disseminated to governmental agencies.
 - CHRI obtained under the Adam Walsh Act or under an NCPA/VCA VECHS program may be disseminated to certain non-governmental entities, such as private schools or private nursing homes, respectively.
 - CHRI received as a result of a Purpose Code H name-based requests under the HOPE Act must not be disseminated to housing agencies.
- Authorized related agencies typically include other agencies/entities involved in a single adjudication or other agencies/entities to which CHRI is shared for authorized re-use.

b. Jurisdictional Control

- CHRI received as a result of fingerprint-based and name-based requests must not be disseminated outside permissible limits of jurisdictional control and agencies/entities outside a jurisdiction cannot be designated as related. Examples of unauthorized dissemination include:
 - A state governmental agency sharing CHRI received under Public Law 92-544 with a governmental agency in another state.
 - Sharing initiatives involving participation in national compacts, associations, or databases.

c. Public Access

- CHRI received as a result of fingerprint-based and name-based requests must not be disseminated to the general public, to include maintaining CHRI formats accessible to the public or releasing CHRI as part of public records requests.
- CHRI may be disclosed at a meeting/hearing open to the public as part of an adjudication process if specific conditions are met.

d. Subject of a Record

- CHRI received as a result of name-based requests must not be disseminated to the subject of the request.
- CHRI received as a result of fingerprint-based requests must only be disseminated to the subject of the record or the subject's attorney. CHRI must not be disseminated to spouses or other household members.
- Applicants must not be given their record and then directed/obligated to provide CHRI to agencies not otherwise permitted to have access.

Next Generation Identification Audit Outline
Noncriminal Justice Access to Criminal History Record Information

3. Purpose for Disclosure of CHRI

a. Reason Fingerprinted (RFP) Field

- The RFP field must accurately reflect the statutory authority and/or the purpose (i.e., applicant type) of the request for CHRI.
- The RFP field must provide a reasonable level of specificity regarding the statutory authority and/or purpose of the request for CHRI (i.e., not overly broad).
 - If an agency is responsible for submitting fingerprints for multiple applicant types (pursuant to one or more statutory authorities), then the RFP field must accurately reflect the single statutory authority and/or purpose corresponding to the specific applicant type, as opposed to the RFP field reflecting all of the possible statutory authorities and/or purposes in each submission.
 - If a single fingerprint submission is made for multiple applicant types, which are known to legitimately exist at the time of submission, then the RFP field must accurately reflect the multiple statutory authorities and/or multiple purposes.

b. Interstate Identification Index (III) Purpose Codes

- The correct purpose code must be used for name-based III queries.

c. Reason for Request

- Reasonably specific supporting information must be provided during audits in order to confirm fingerprint-based and name-based requests for CHRI are for authorized purposes.
- Reasonably specific supporting information must be provided during audits in order to confirm the accuracy of the RFP field and correct III purpose code usage.

4. Applicant Notification and Record Correction

a. Privacy Act Statement

- All applicants (i.e. subjects of a request for CHRI) must be provided a written FBI Privacy Act statement or substantively similar language (2013 version or later).

b. Procedures to Correct a Record

- All applicants (i.e. subjects of a request for CHRI) must be provided written notice regarding procedures for accessing and correcting their FBI record (found at Title 28, Code of Federal Regulations, Section 16.34).

c. Opportunity to Correct a Record

- All applicants (i.e. subjects of a request for CHRI) must be provided the opportunity to correct their FBI records (if such records exist) regardless of the record's effect on the outcome of the adjudication.

Next Generation Identification Audit Outline
Noncriminal Justice Access to Criminal History Record Information

5. User Fee

a. Criminal Justice

- Fingerprint checks for screening criminal justice agency employees or applicants for employment (sworn and non-sworn) may be submitted as no-fee type of transactions.
- Fingerprint checks for screening those under contract with a criminal justice agency, where the contractor is performing services for the administration of criminal justice, may be submitted as no-fee type of transactions.
- Fingerprint checks for screening those under contract with a criminal justice agency, where the contractor is not performing services for the administration of criminal justice but has unsupervised access to the facility, may be submitted as no-fee type of transactions.
- Fingerprint checks for screening employees of contractors to whom an entire administration of criminal justice function has been outsourced, such as a private prison or dispatch center, must be submitted as full user fee type of transactions.

b. Volunteer

- Fingerprint checks for screening noncriminal justice applicants, who are not volunteering to provide care for children, the elderly, or individuals with disabilities, must be submitted at the full user fee rate.
- Fingerprint checks for screening volunteers, who provide care for children, the elderly, or individuals with disabilities, may be submitted at the reduced user fee rate (Type of Search Request value of “V”).

**NEVADA CRIMINAL
JUSTICE INFORMATION
ADMINISTRATIVE
POLICIES**

Section 10

NONCRIMINAL JUSTICE AUTHORIZED RECIPIENTS

10.1 General

The Central Repository for the Nevada Records of Criminal History is housed within the Nevada Department of Public Safety, Records, Communications and Compliance Division (RCCD). The Central Repository is responsible for providing Noncriminal Justice Authorized Recipients with access to Criminal History Record Information (CHRI), as authorized by legislative enactment or federal executive order based on fingerprint-based background checks for licensing, employment, or other noncriminal justice purposes.

The National Crime Prevention and Privacy Compact Council works in partnership with criminal history record custodians, end users, and policy makers to regulate and facilitate the sharing of complete, accurate, and timely CHRI to noncriminal justice users in order to enhance public safety, welfare, and the security of society while recognizing the importance of individual privacy rights. This is facilitated in part through the development of resource materials for use in protecting criminal justice information from unauthorized and inappropriate access, collection, maintenance and disclosure. Within the Central Repository, the Nevada Criminal Justice Information System (NCJIS) Compliance Unit (NCU) performs several duties in regard to compliance with the federal and state statutes and regulations for noncriminal justice agencies' access to CHRI:

- Training on the use of CHRI
- Conducting audits
- Researching/investigating security breaches

10.2 Authority to Access CHRI

1. Each Authorized Recipient requesting access to receive fingerprint-based CHRI must submit its authorizing state statute, county/city ordinance, or federal authority for review to the Central Repository through the application process found in Section 10.
2. Certain statutory and/or federal authority requires training prior to being granted access to CHRI.
3. The Central Repository may charge a fee in accordance with applicable law for handling a request involving fingerprint processing for noncriminal justice purposes per Nevada Revised Statute 179A. Pursuant to Public Law 101-515 the FBI may establish and collect fees to process fingerprint identification records and name checks for noncriminal justice, non-law enforcement uses, in accordance with Title 42, United State Code. Authorized Recipients must ensure that all fingerprint-based requests for CHRI are properly submitted in order to ensure appropriate fee.

10.3 User Agreements

All Authorized Recipients that have been approved for access to CHRI must sign a User Agreement with the Department of Public Safety (DPS), Central Repository and are legally bound thereby and agree to abide by all provisions contained therein. The contract serves to identify the responsibilities between the CJIS Systems Agency (CSA) and the Noncriminal Justice Authorized Recipients.

- a. Authority and Purpose: It is prohibited for noncriminal justice and criminal justice Authorized Recipient to use CHRI for any purpose other than that for which it was requested.
 - b. Authorized Personnel: Employees who have access or proximity to CHRI and who are employed by the Authorized Recipient.
 - c. Authorized Recipient: Government/Nongovernmental, private for profit/non-profit agency authorized by federal statute, federal executive order, or has been approved by the United States Attorney General pursuant to Public Law 92-544 to receive CHRI for noncriminal justice purposes.
 - The Authorized Recipient must designate an individual as a Point of Contact (as defined herein) in addition to a group of individuals to receive CHRI for noncriminal justice functions associated with civil fingerprint submissions. This can include, but is not limited to, the Records Custodian or Hiring Authority responsible for determining the hiring and/or suitability of the applicant based on the fingerprint response.
 - d. Point of Contact (POC): An employee of the Authorized Recipient who shall act as the designated liaison between the Authorized Recipient and the CSA.
 - e. Policies/Procedures: Authorized Recipient must implement policies and procedures which provide for the security and proper handling of the CHRI. As a best business practice agencies should also have rules for fingerprint submissions which include proper applicant identification and protecting the fingerprint card from tampering.
 - f. Training: Each criminal or Noncriminal Justice Authorized Recipient is responsible to train on the security and proper handling of CHRI for any additional personnel based on the required internal written policies/procedures.
1. User Agreement shall be reviewed during compliance audits by the NCJIS Compliance Unit audit staff. The agreement shall remain in force until:
 - a. Authorized Recipient violates any portion of the agreement or policies which result in the termination of said access; OR

- b. Authorized Recipient advises the Central Repository in writing of the Authorized Recipient wish to cancel access; OR
- c. Until renewed by the Central Repository

10.4 Outsourcing Responsibilities

Outsourcing is available to all agencies excluding those using the NCPA/VCA (National Child Protection Act of 1993 as amended by the Volunteers for Children Act) as their statutory authority to submit fingerprints to the Central Repository. If an agency chooses to outsource their duties or store CHRI offsite then Attachment A: Security and Management Control Outsourcing Standard for Non-Channelers, and Attachment B: Responsibility Table for Non-channeling must be followed.

Authorized Recipient shall provide the Department of Public Safety's Central Repository with a written request to outsource, and the Central Repository will approve or disapprove with a return letter to the agency prior to outsourcing.

Note: Failure to seek approval prior to outsourcing noncriminal justice duties can result in account suspension.

10.5 Responsibilities of the Authorized Recipient (AR)

The POC is designated as the primary liaison between their Authorized Recipient and the Central Repository, and is responsible for coordinating agency compliance pertaining to the access, use, handling, dissemination and destruction of CHRI.

1. Must complete mandatory training set by the Central Repository.
2. Serves as the central contact point to the Central Repository.
3. Must immediately notify the Central Repository of any intentional misuse of CHRI.
4. Any new, updated or changed authority by state statute, county ordinance or municipal code must be submitted to the Central Repository for approval prior to submitting fingerprints.

Note: Failure to seek approval prior to updating or implementing new authorities can result in account suspension.

5. Maintain an authorized personnel list of authorized recipient personnel who are part of the determination group. A determination group is defined as any Authorized Recipient personnel who play a part in making the determination for suitability or eligibility to work or volunteer for the criminal justice or noncriminal justice Authorized Recipient.
6. Ensure all personnel have met all training requirements as specified in section 10 of this policy.
7. FBI applicant privacy rights notification must be provided to applicant in writing per Title 28

Code of Federal Regulations 50.12(b), the Fingerprint Background Waiver must be signed and dated prior to any applicant being fingerprinted. This waiver advises the applicant of the following:

- a. Fingerprints will be used to check the criminal history records of the State and the FBI.
- b. Informs the applicant that they are allowed a reasonable opportunity to complete and challenge the accuracy of the criminal history record.
- c. Notifies the applicant on how to obtain a copy of their FBI record of criminal history pursuant to Title 28 CFR Section 16.34.

Note: This waiver must be maintained on file for one complete audit cycle. The FBI's audit cycle is every 3 years from the previous FBI audit and the State's audit cycle is every 5 years from the last state audit.

8. The applicant must sign and date the Notice to Applicant Waiver prior to the Authorized Recipient submitting the applicant's fingerprints under the authority of the NCPA/VCA. This waiver contains the following information:
 - a. Name, address and date of birth appearing on a valid identification document of the applicant (as defined in section 1028 of Title 18, United States Code).
 - b. Certification that applicant has not been convicted of a crime and, if the applicant has been convicted of a crime, contains a description of the crime and the particulars of the conviction.
 - c. Notifies the applicant that their fingerprints will be used to check the criminal history records of the state and FBI.
 - d. Notifies the applicant of their right to challenge the accuracy and completeness of the CHRI.
 - e. Notifies the applicant that the Authorized Recipient may deny the applicant's unsupervised access to the Authorized Recipients clientele pending the completion of the background check.
9. Cooperate and give assistance to the Central Repository's audit staff with required or directed compliance audits.
10. Notify the Central Repository within 10 calendar days when changes occur in the Authorized Recipient's name, contact person, mailing address, email address and/or phone number.

10.6 Termination of Access to State and FBI Responses

1. The CSO may suspend or terminate an Authorized Recipient's access to CHRI for a violation

of the User Agreement. In addition, any violation of NCJIS, state or federal statutes, regulations or rules incorporated in the Noncriminal Justice and Criminal Justice Authorized Recipient shall be deemed a breach of terms.

2. An Authorized Recipient may terminate access to CHRI with written notice to the Central Repository.

10.7 Security and Training Requirements

Criminal and Noncriminal Justice Authorized Recipients must have written policies and procedures regarding access, use, dissemination, and disposal of fingerprint-based CHRI.

1. Physical Security-Authorized Recipient is responsible for the security of the CHRI from its arrival with the Authorized Recipient through the point of its destruction. This includes maintaining the CHRI in a secure location that is not readily accessible to individuals not authorized to see it (i.e., locked file cabinet, locked room, etc.).
2. Technical Security-Fingerprint-based CHRI stored electronically or CHRI obtained from the fingerprint results and stored electronically by means of logs, or letters would dictate the Authorized Recipient then becomes subject to the FBI CJIS technical requirements and an audit conducted by the Central Repository's Information Security Officer.
3. Personnel Security-All persons directly associated with the accessing, maintaining, processing, dissemination or destruction of CHRI shall be trained on the handling of the information.
4. Authorized personnel must complete one of the following two types of training:
 - a. CJIS Online Training: CJIS Online is the minimum basic Security Awareness training required for all individuals (criminal justice and noncriminal justice) who view or handle criminal history information. All authorized personnel must receive CJIS Online training within six months of hire or being placed on the authorized personnel list and then every two years thereafter.
 - b. Training Acknowledgement: The Authorized Recipient must keep a record that each authorized person who has access to CHRI has been trained on the following. The acknowledgment must be maintained, reviewed, signed and kept on file for as long as each person is authorized.
 - i. CHRI cannot be disseminated outside the receiving department, related agencies, or other authorized entities.
 - ii. CHRI must be maintained in a secured records environment.
 - iii. CHRI must be destroyed by shredding or burning.
 - iv. Penalties for misuse of the information.

5. **Destruction:** When no longer needed for its purpose, CHRI should be destroyed to minimize the risk of unauthorized access and dissemination. The acceptable methods of destruction are shredding, or burning. Destruction must be performed or observed by personnel who are authorized to access/handle CHRI. Each Authorized Recipient should check its records retention policies with its regulatory or auditing bodies before destroying CHRI.

10.8 Dissemination

CHRI must be used solely for the purpose requested and cannot be disseminated outside the receiving departments, related Authorized Recipients or other authorized entities. Verbal or written communication regarding CHRI may only occur between personnel authorized to possess the information and carry out the specific purpose for which the information was requested.

1. **Subject of the Record:** Authorized Recipient may disseminate fingerprint-based CHRI to the subject of the record (i.e., the applicant) for the subject to challenge their criminal history records. If that is the case, the Authorized Recipients must stamp the word “copy” in red on each page of the provided records, a secondary dissemination log must be maintained, and the log must contain the following information:
 - a. The date the information was provided to the subject of the record.
 - b. The subject of the record’s name.
 - c. A description of the information that was disseminated (State Background Check or National Background Check).
 - d. To whom the record is being disseminated to (only the applicant).
 - e. How is the record being disseminated (i.e. Verbally, person, or writing).

Note: It is considered best business practice for the Authorized Recipient to include the steps it took to validate the applicant’s identity, if the Authorized Recipient is disseminating the record in person. If the CHRI is being mailed using the U.S. Postal Service, this should also be indicated. CHRI may not be disseminated to spouses, other household, or family members, or attorneys even at the applicant’s request.

2. **Notifications/ Public Access:** CHRI received from fingerprints are not public record and may not be released to the public. The Authorized Recipient may neither confirm nor deny the existence or nonexistence of an individual’s criminal history record to the public or to any unauthorized individual or Authorized Recipient. Generic met or did not meet eligibility requirements language must be used to the greatest extent possible, with the understanding that a reasonable balance must exist between the need to notify and not indirectly confirming the existence or non-existence of CHRI.
3. **Jurisdictional Control:** Authorized Recipients outside of the State of Nevada will not be designated as Authorized Recipients of fingerprint-based CHRI, even when a congruent related

need appears to exist for the use of CHRI. Each state has its own statutory authorities that must be followed. Authorized Recipients are not allowed to forward fingerprint CHRI to another state, even if the Authorized Recipient has additional out of state offices.

10.9 Audit

1. Authorized Recipients that receive CHRI directly from the Central Repository will be audited every five years by the Central Repository's audit staff. A notification will be sent with a description of the audit process along with the compliance information. Compliance auditors will conduct a review of the Authorized Recipients prior to the audit interview. All documentation relating to general administration, fingerprint submissions, privacy security, and training will be reviewed at the audit.
2. After an audit has been completed, auditors will provide the Authorized Recipients with a written report which will either denote complete compliance or will contain recommendations for corrective actions to bring the agency into compliance.
3. Directed audits will be conducted as necessary. A directed audit is defined as an audit that is conducted as a result of an incident/allegation or a request received by the CSA.

10.10 Audit Plan

The Audit Plan focuses on ten areas of agency accountability which are as follows:

1. Authority and use of CHRI.
2. Dissemination of CHRI.
3. Personnel Training Standards.
4. Applicant Notification and Record Challenge.
5. Privacy and Security of CHRI.
6. Outsourcing of Noncriminal Justice Administrative Functions.
7. User Agreement.
8. Authorized Personnel List.
9. Authorized Recipient Account Information.
10. Internal Written Procedures.

10.11 Discipline and Sanctions

The CSA has developed a three-phase sanction plan that will be initiated whenever an Authorized Recipient is not in compliance with NCJIS and FBI CJIS policies and procedures. This process will enhance system integrity and security through increased user compliance.

PHASE 1

1. An audit report will be sent to the attention of the AR for review and immediate corrective action.
2. A written formal response detailing the compliance resolution from the Authorized Recipient shall be directed to the assigned auditor within the Central Repository within 30 business days of the audit report. The agency's formal response must include the following issues:
 - a. Noncompliance issues cited in the audit.
 - b. Documentation of corrective measures.
 - c. Corrective measures will be implemented to eliminate future noncompliance
3. If noncompliance remains an issue, Phase 2 will be initiated at the discretion of the CSO.

PHASE 2

1. A letter from the CSA will be forwarded to the AR outlining the result of the noncriminal justice audit and the Authorized Recipient's failure to implement corrective measures. This letter will request a meeting with the head of the AR regarding implementation of limited noncriminal justice services for the subject agency.
2. Limited sanctions that may be initiated at this time are:
 - a. Suspended access to CHRI.
 - b. 60 days probation, which may include requirements for the Authorized Recipient to provide additional documentation.
3. If noncompliance remains an issue, Phase 3 will be initiated at the discretion of the CSO.

PHASE 3

1. A letter from the Director of the Department of Public Safety will be forwarded to the AR advising that noncriminal justice services to that Authorized Recipient have been terminated. This letter will address the Authorized Recipient's deficiencies as noted in the audit, the Authorized Recipient's failure to implement appropriate corrective measures and previously imposed sanctions.

2. All action taken by the Department of Public Safety will be documented and maintained at the Central Repository.

REINSTATEMENT OF NCJIS SERVICES

1. To regain access to CHRI services, a formal letter from the AR must be submitted to the CSA. All of the following issues must be addressed:
 - a. Noncompliance issues that initiated the enforced sanctions.
 - b. Implemented plans to ensure compliance in the future.
 - c. Requested date for re-inspection by the Central Repository.
2. Upon completion of a satisfactory re-inspection by Central Repository personnel, the Authorized Recipient's original level of access will be restored.
3. The Authorized Recipients will be placed on probation at the discretion of the CSO and areas of noncompliance will be monitored.

APPENDIX A

TERMS AND DEFINITIONS

Access to Criminal Justice Information – The physical or logical (electronic) ability, right or privilege to view, modify or make use of Criminal Justice Information.

Administrative Messages (AM) – A secure and documentable means of interagency communication. An AM may be used for any type of official law enforcement or public safety purpose as approved by Nlets and NCIC.

Agency Administrator (AA) – An individual located within an agency that is ultimately responsible for security and compliance requirements.

Aggregate – A form by the conjunction or collection of particulars into a whole mass or sum; total; combined. A whole formed by combining several elements.

Assistant Terminal Agency Coordinator (ATAC) – An individual located within an agency designated to assist the terminal agency coordinator as liaison between the agency and the CSA.

AUTHORIZED RECIPIENT (Civil Accounts) - (1) A non-governmental entity authorized by federal statute or federal executive order to receive CHRI for noncriminal justice purposes, or (2) a government agency authorized by federal statute, federal executive order, or state statute which has been approved by the United States Attorney General pursuant to Public Law 92-544 to receive CHRI for noncriminal justice purposes.

AUTHORIZED RECIPIENT (NCPA/VCA accounts) - A governmental, public, private, for-profit, or not-for-profit entity operating within the State of Nevada authorized to submit fingerprints and review resultant CHRI as part of the screening process for current and/or prospective employees, volunteers, contractors and vendors who have or may have unsupervised access to children, the elderly or disabled persons for whom Authorized Recipient provides services or care.

Authorized Personnel – An individual, or group of individuals, who have been appropriately vetted (national and state fingerprint-based record check, a wants/warrant check and received appropriate training) and have been granted access to CJI.

Certification – The action or process of providing someone or something with an official document attesting to a status or level of achievement.

CJIS Security Officer (CSO) – An individual located within the CSA responsible for the administration of FBI CJIS programs for the CSA.

CJIS Security Policy – The FBI CJIS Security Policy document as published by the FBI CJIS Information Security Officer.

CJIS System Agency (CSA) – A state criminal justice agency providing access to its criminal justice users with respect to FBI CJIS data. There can only be one CSA per state.

Confidentiality – The concept of ensuring that information is observable only to those who have been granted authorization to do so.

Contractor – A private business, agency or individual which has entered into an agreement for the administration of criminal justice or noncriminal justice functions with a Criminal Justice or a Noncriminal Justice Agency.

Criminal History Record Information (CHRI) – A subset of CJI. Any notations or other written or electronic evidence of an arrest, detention, complaint, indictment, information or other formal criminal charge relating to an identifiable person that includes identifying information regarding the individual as well as the disposition of any charges.

Criminal Justice Information (CJI) – Criminal Justice Information is the abstract term used to refer to all of the NCJIS and FBI CJIS provided data necessary for law enforcement agencies to perform their mission and enforce the laws, including but not limited to: biometric, identity history, person, organization, property, and case/incident history data. In addition, CJI refers to the NCJIS and FBI CJIS-provided data necessary for noncriminal justice agencies to perform their mission; including, but not limited to data used to make hiring decisions.

Criminal Justice Information Services Division (FBI CJIS or CJIS) — The FBI division Responsible for the collection, warehousing, and timely dissemination of relevant CJI to the FBI and to qualified law enforcement, criminal justice, civilian, academic, employment, and licensing agencies.

Criminal Justice Practitioner – A non-sworn or non-terminal operator that could receive or view hard copy NCJIS/NCIC record information.

Data – Facts and statistics collected for reference or analysis.

Direct Access – (1) Having the authority to access systems managed by NCJIS and the FBI CJIS Division, whether by manual or automated methods, not requiring the assistance of, or intervention by, any other party or agency (28 CFR, Part 20). (2) Having the authority to query or update national databases maintained by NCJIS and the FBI CJIS Division including national queries and updates automatically or manually generated by the CSA.

Dissemination –Disclosing records of criminal history or the absence of records of criminal history to a person or agency outside the organization which has control of the information.

Escorting – An unauthorized person in a physically secure area must be escorted by a person who is sufficiently familiar with the equipment in the area and the tasks being performed. The escort must be able to identify an unauthorized act and alert security personnel. If the escort does not have this set of knowledge and skills, then the person cannot be an escort.

Federal Bureau of Investigation (FBI) - The FBI is a government agency in the United States that investigates crimes in which a national law is broken or in which the country's security is threatened.

Information Security Officer (ISO) – An individual designated by the CSO who has the responsibilities to establish and maintain information security policy, assesses threats and vulnerabilities, performs risk and control assessments, oversee the governance of security operations and establishes information security training and awareness programs. The ISO interfaces with security operations to manage implementation details and with auditors to verify compliance with established policies.

Interlocal Contract – See User Agreement

Internal Written Procedures (IWP) – An Agency’s written procedures detailing how a policy will be implemented

Interstate Identification Index (III) – A national index-pointer system of criminal histories (rap sheet) in the United States, managed by the FBI at the National Crime Information Center.

JLink – Nevada’s current message switch, which stands for “Justice Link.” Justice Link is the “Windows-based” system that NCJIS users access to perform their criminal justice functions.

LEOKA - The data collected under the auspices of the Law Enforcement Officers Killed and Assaulted (LEOKA) Program involves law enforcement officers who meet a certain set of criteria established by the FBI.

Law Enforcement National Data Exchange (N-DEx) – FBI CJIS division system providing law enforcement agencies with a shared investigative tool. For further reference see the Audit Section of this Manual.

Local Agency Security Officer (LASO) – A point-of-contact designated as the liaison between their agency and the ISO who has access to the NCJIS network and provides any needed technical systems assistance to help assure the confidentiality, integrity and availability of criminal justice information on the network.

National Crime Information Center (NCIC) – FBI information system which stores CJI which can be queried by appropriate Federal, state and local law enforcement, criminal justice and certain noncriminal justice agencies.

Nevada Criminal Justice Information System (NCJIS) – Nevada’s primary criminal justice information system that houses and provides for the expeditious exchange of criminal justice information between Local, State and Federal agencies.

National Incident-Based Reporting System (NIBRS) - National Incident-Based Reporting System is an incident-based reporting system used by law enforcement agencies in the United States for collecting and reporting data on crimes. Local, state and federal agencies generate NIBRS data from their records management systems.

Nlets – The International Justice and Public Safety Network. Previously known as the National Law Enforcement Telecommunications System.

Non-Terminal Agency (NTA) – An agency having access to NCJIS/NCIC information through a terminal agency.

Non-Terminal Agency Coordinator (NTAC) - An individual located within an agency designated as the liaison between their agency and the CSA. The TAC administers NCJIS/CJIS systems programs within the local agency and oversees the agency's compliance with those policies.

NRS – Nevada Revised Statutes

NCJIS Compliance Unit (NCU) - Manages, trains and audits Users of the NCIC/NCJIS systems, Civil Applicant, Civil Name Check and the Uniform Crime Reporting (UCR) program. Serves as the CJIS Systems Agency (CSA) for the State which includes the National Crime Information Center (NCIC), Interstate Identification Index (III), and Nlets.

Originating Agency Identifier (ORI) – A unique alpha numerical identifier authorized by the CSA.

Point of Contact - An employee of the Authorized Recipient who shall act as the designated liaison between the Authorized Recipient and the CSA.

Physically Secure Location – A facility or an area, a room, or a group of rooms, within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems.

Record Management System (RMS) - Is the management of records for an organization throughout the records-life cycle. The activities in this management include the systematic and efficient control of the creation, maintenance, and destruction of the records along with the business transactions associated with them.

Reporting Agency Coordinator (RAC) –UCR Agency Coordinator is responsible for promoting the program and managing all the activities relating to their agency. These activities include assisting employees with understanding how the program works and acting as the central information contact for the agency.

Retention - A **records retention** schedule is a policy that defines how long data items must be kept.

Secondary Dissemination – The release of CHRI from one agency to an authorized recipient agency when the recipient agency's ORI was not used to run the transaction.

Summary Reporting System (SRS) – The national method of collecting uniform crime reporting statistics for the FBI since the 1930's.

Terminal Agency (TA) – An agency that has direct computer access to the NCJIS/NCIC system.

Terminal Agency Coordinator (TAC) – An individual located within an agency designated as the liaison between their agency and the CSA. The TAC administers NCJIS/CJIS systems Programs within the local agency and oversees the agency's compliance with those policies.

Terminal Operator – An individual, that transmits, receives and coordinates information through direct communication to the NCJIS system (NCJIS, NCIC, and Nlets) and ensures their agency's compliance with state and federal regulations for the use of the systems.

Uniform Crime Reporting (UCR) - The UCR Program collects statistics on the number of criminal offenses known to law enforcement.

Uniform Crime Reporting Program - A collective effort on the part of the city, county, state, and federal law enforcement agencies to present a nationwide view of crime.

User Agreement – An User Agreement/Interlocal Contract is a legally binding document. The User Agreement identifies the responsibilities between servicing agencies.

Vendor - Is a party in the supply chain that makes goods and services available to companies or consumers

U. S. Department of Justice

Federal Bureau of Investigation

Criminal Justice Information Services Division



Criminal Justice Information Services (CJIS) Security Policy

Version 6.0

12/27/2024



Prepared by:
FBI CJIS Information Security Officer

Approved by:
CJIS Advisory Policy Board

EXECUTIVE SUMMARY

Criminal and noncriminal justice agencies need timely and secure access to services that provide data wherever and whenever for stopping and reducing crime. In response to these needs, the Advisory Policy Board (APB) recommended to the Federal Bureau of Investigation (FBI) that the Criminal Justice Information Services (CJIS) Division authorize the expansion of the existing security management structure in 2019. Administered through a shared management philosophy, the CJIS Security Policy (CJISSECPOL) contains information security requirements, guidelines, and agreements reflecting the will of law enforcement and criminal justice agencies for protecting the systems that process, store, and transmit Criminal Justice Information (CJI). The Federal Information Security Management Act of 2014 provides further legal basis for the APB approved management, operational, and technical security requirements mandated to protect CJI and by extension the hardware, software and infrastructure required to enable the services provided to the criminal and noncriminal justice communities.

The essential premise of the CJISSECPOL is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CJISSECPOL provides guidance for the creation, viewing, modification, transmission, dissemination, storage, or destruction of CJI. This Policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal and noncriminal justice services and information.

The CJISSECPOL integrates presidential directives, federal laws, FBI directives and the criminal and noncriminal justice community decisions along with guidance from the National Crime Prevention and Privacy Compact Council (Compact Council). The Policy is presented at both strategic and tactical levels and is periodically updated to reflect the security requirements of evolving technology and business models. The Policy features modular sections enabling more frequent updates to address emerging threats and new security measures. The provided security criteria assists agencies with designing and implementing systems to meet a minimum level of risk and security protection while enabling agencies the latitude to institute more stringent security requirements and controls based on their business model and local needs.

The CJISSECPOL strengthens the partnership between the FBI and CJIS Systems Agencies (CSA), including, in those states with separate authorities, the State Identification Bureaus (SIB), and Interface Agencies (IA). Further, as use of criminal history record information (CHRI) for noncriminal justice purposes continues to expand, the CJISSECPOL becomes increasingly important in guiding the National Crime Prevention and Privacy Compact Council and State Compact Officers in the secure exchange of CHRI.

The Policy describes the vision and captures the security concepts that set the policies, protections, roles, and responsibilities with minimal impact from changes in technology. The Policy empowers CSAs, SIBs, and IAs with the insight and ability to tune their security programs according to their risks, needs, budgets, and resource constraints while remaining compliant with the baseline level of security set forth in this Policy. The CJISSECPOL provides a security framework based on laws, standards, and elements of published and vetted policies for accomplishing the mission across the broad spectrum of the criminal justice and noncriminal justice communities.

CHANGE MANAGEMENT

Revision	Change Description	Created/Changed by	Date	Approved By
6.0	Policy Modernization Completion	Security Policy Modernization Task Force	12/27/2024	APB & Compact Council

SUMMARY OF CHANGES

Version 6.0

APB Approved Changes

1. **Modernizing the Executive Summary, Section 1: Introduction, Section 2: *CJISSECPOL* Approach, and Section 3: Roles and Responsibilities in the *CJISSECPOL*, Spring 2024, APB#11, SA#2:** update sections with approved changes.
2. **Changing and Refreshing Authenticators in the *CJISSECPOL*, Spring 2024, APB#11, SA#3:** clarifies which authenticator type requires annual changing and clarifies the use of a “banned password” list.
3. **Modernizing System and Services Acquisition (SA) in the *CJISSECPOL*, Spring 2024, APB#11, SA#5:** add definitions and modernize the CJIS Security Policy requirements for:

- System and Services Acquisition Policy and Procedures**
- Allocation of Resources**
- System Development Lifecycle**
- Acquisition Process**
- System Documentation**
- Security and Privacy Engineering Principles**
- External System Services**
- Developer Configuration Management**
- Developer Testing and Evaluation**
- Developer Process, Standards, and Tools**

4. **Modernizing Supply Chain and Risk Management (SR) in the *CJISSECPOL*, Spring 2024, APB#11, SA#6:** modernize the CJIS Security Policy requirements for

- Supply Chain Risk Management Policy and Procedures**
- Supply Chain Risk Management Plan**
- Acquisition Strategies, Tools, and Methods**
- Notification Agreements**
- Inspection of Systems or Components**
- Component Disposal**

5. **Modernizing Personnel Security (PS) in the *CJISSECPOL*, Spring 2024, APB#11, SA#7:** modernize the CJIS Security Policy requirements for

- Personnel Security Policy and Procedures**
- Position Risk Designation**
- Personnel Screening**
- Personnel Termination**
- Personnel Transfer**
- Access Agreements**
- External Personnel Security**

**Personnel Sanctions
Position Descriptions**

6. **Modernizing Assessment, Authorization, and Monitoring (CA) in the *CJISSECPOL*, Spring 2024, APB#11, SA#8:** modernize the CJIS Security Policy requirements for

**Assessment, Authorization, and Monitoring Policy and Procedures
Control Assessments
Information Exchange
Plan of Action and Milestones
Authorization
Continuous Monitoring
Internal System Connections**

7. **Remove Appendix J and K from the *CJISSECPOL*, Spring 2024, APB#11, SA#9:** remove the indicated appendices.

Administrative Changes

1. There are no Administrative Changes in this version.

Note: Administrative changes are vetted through the Security and Access Subcommittee and not the entire APB process.

KEY TO APB APPROVED CHANGES (e.g., “Section 5.13 Mobile Devices, Fall 2013, APB#11, SA#6, Future CSP for Mobile Devices: add language”):

Section Number and Name

Fall 2013 – Advisory Policy Board cycle and year

APB# – Advisory Policy Board Topic number

SA# – Security and Access Subcommittee Topic number

Topic Paper Title

Summary of change

TABLE OF CONTENTS

Executive Summary	i
Change Management.....	ii
Summary of Changes.....	iii
Table of Contents	v
List of Figures.....	xv
List of Priorities.....	xvi
1 Introduction.....	1
1.1 Purpose.....	1
1.2 Scope.....	1
1.3 Relationship to Local Security Policy and Other Policies	1
1.4 Terminology Used in This Document.....	1
1.5 Distribution of the CJIS Security Policy.....	2
2 CJIS Security Policy Approach	3
2.1 CJIS Security Policy Vision Statement.....	3
2.2 Architecture Independent.....	3
2.3 Risk Versus Realism	3
3 Roles and Responsibilities	4
3.1 Shared Management Philosophy.....	4
3.2 Roles and Responsibilities for Agencies and Parties	4
3.2.1 CJIS Systems Agencies (CSA)	5
3.2.2 CJIS Systems Officer (CSO).....	5
3.2.3 Terminal Agency Coordinator (TAC).....	6
3.2.4 Criminal Justice Agency (CJA).....	6
3.2.5 Noncriminal Justice Agency (NCJA).....	6
3.2.6 Contracting Agency (CA)	7
3.2.7 Agency Coordinator (AC).....	7
3.2.8 CJIS Systems Agency Information Security Officer (CSA ISO)	7
3.2.9 Organizational Personnel with Security Responsibilities	8
3.2.10 FBI CJIS Division Information Security Officer (FBI CJIS ISO)	8
3.2.11 Repository Manager	8
3.2.12 IA Official	9
3.2.13 State Compact Officer (SCO)	9
4 Criminal Justice Information and Personally Identifiable Information	10
4.1 Criminal Justice Information (CJI)	10
4.1.1 Criminal History Record Information (CHRI).....	10
4.2 Access, Use and Dissemination of Criminal History Record Information (CHRI), NCIC Restricted Files Information, and NCIC Non-Restricted Files Information.....	11
4.2.1 Proper Access, Use, and Dissemination of CHRI	11
4.2.2 Proper Access, Use, and Dissemination of NCIC Restricted Files Information.....	11
4.2.3 Proper Access, Use, and Dissemination of NCIC Non-Restricted Files Information 11	
4.2.3.1 For Official Purposes	11
4.2.3.2 For Other Authorized Purposes	12
4.2.3.3 CSO Authority in Other Circumstances	12

4.2.4	Storage.....	12
4.2.5	Justification and Penalties	12
4.2.5.1	Justification	12
4.2.5.2	Penalties	12
4.3	Personally Identifiable Information (PII).....	12
5	Policy and Implementation	14
5.1	Policy Area 1: Information Exchange Agreements	15
5.1.1	Information Exchange	15
5.1.2	Monitoring, Review, and Delivery of Services	15
5.1.2.1	Managing Changes to Service Providers	15
	ACCESS CONTROL (AC)	16
	AC-1 Policy and Procedures	16
	AC-2 Account Management	17
	(1) Account Management Automated System Account Management.....	20
	(2) Account Management Automated Temporary and Emergency Account Management	20
	(3) Account Management Disable Accounts	20
	(4) Account Management Automated Audit Actions	20
	(5) Account Management Inactivity Logout.....	21
	(13) Account Management Disable Accounts for High-Risk Individuals	21
	AC-3 Access Enforcement.....	21
	(14) Access Enforcement Individual Access.....	22
	AC-4 Information Flow Enforcement.....	22
	AC-5 Separation of Duties.....	23
	AC-6 Least Privilege.....	24
	(1) Least Privilege Authorize Access to Security Functions.....	24
	(2) Least Privilege Non-Privileged Access for Nonsecurity Functions	24
	(5) Least Privilege Privileged Accounts.....	25
	(7) Least Privilege Review of User Privileges	25
	(9) Least Privilege Log Use of Privileged Functions.....	25
	(10) Least Privilege Prohibit Non-Privileged Users from Executing Privileged Functions	26
	AC-7 Unsuccessful Logon Attempts	26
	AC-8 System Use Notification	27
	AC-11 Device Lock	28
	(1) Device Lock Pattern-Hiding Displays.....	28
	AC-12 Session Termination.....	28
	AC-14 Permitted Actions without Identification or Authentication.....	29
	AC-17 Remote Access	29
	(1) Remote Access Monitoring and Control	30
	(2) Remote Access Protection of Confidentiality and Integrity Using Encryption.....	30
	(3) Remote Access Managed Access Control Points	31
	(4) Remote Access Privileged Commands and Access.....	31
	AC-18 Wireless Access	31
	(1) Wireless Access Authentication and Encryption.....	32
	(3) Wireless Access Disable Wireless Networking.....	32

AC-19 Access Control for Mobile Devices	32
(5) Access Control for Mobile Devices Full Device or Container-Based Encryption	33
AC-20 Use of External Systems	33
(1) Use of External Systems Limits On Authorized Use	34
(2) Use of External Systems Portable Storage Devices — Restricted Use	35
AC-21 Information Sharing	35
AC-22 Publicly Accessible Content	36
AWARENESS AND TRAINING (AT)	37
AT-1 Policy and Procedures	37
AT-2 Literacy Training and Awareness	38
(2) Literacy Training and Awareness Insider Threat	39
(3) Literacy Training and Awareness Social Engineering and Mining	39
AT-3 Role-Based Training	40
(5) Role-Based Training Processing Personally Identifiable Information	42
AT-4 Training Records	43
AUDIT AND ACCOUNTABILITY (AU)	45
AU-1 Policy and Procedures	45
AU-2 Event Logging	46
AU-3 Content of Audit Records	47
(1) Content of Audit Records Additional Audit Information	48
(3) Content of Audit Records Limit Personally Identifiable Information Elements	49
AU-4 Audit Log Storage Capacity	49
AU-5 Response to Audit Logging Process Failures	49
AU-6 Audit Record Review, Analysis, and Reporting	50
(1) Audit Record Review, Analysis, and Reporting Automated Process Integration	50
(3) Audit Record Review, Analysis, and Reporting Correlate Audit Record Repositories	51
AU-7 Audit Record Reduction and Report Generation	51
(1) Audit Record Reduction and Report Generation Automatic Processing	51
AU-8 Time Stamps	52
AU-9 Protection of Audit Information	52
(4) Protection of Audit Information Access by Subset of Privileged Users	53
AU-11 Audit Record Retention	53
AU-12 Audit Record Generation	54
ASSESSMENT, AUTHORIZATION, AND MONITORING (CA)	55
CA-1 Policy and Procedures	55
CA-2 Control Assessments	56
(1) Control Assessments Independent Assessors	57
CA-3 Information Exchange	58
CA-5 Plan of Action and Milestones	61
CA-6 Authorization	61
CA-7 Continuous Monitoring	62
(1) Continuous Monitoring Independent Assessment	64
(4) Continuous Monitoring Risk Monitoring	64
CA-9 Internal System Connections	64
CONFIGURATION MANAGEMENT (CM)	66

CM-1 Policy and Procedures	66
CM-2 Baseline Configuration	67
(2) Baseline Configuration Automation Support for Accuracy and Currency	67
(3) Baseline Configuration Retention of Previous Configurations	68
(7) Baseline Configuration Configure Systems and Components for High-Risk Areas ..	68
CM-3 Configuration Change Control	69
(2) Configuration Change Control Testing, Validation, and Documentation of Changes	69
(4) Configuration Change Control Security and Privacy Representatives	70
CM-4 Impact Analyses	70
(2) Impact Analyses Verification of Controls	71
CM-5 Access Restrictions for Change	71
CM-6 Configuration Settings	71
CM-7 Least Functionality	72
(1) Least Functionality Periodic Review	73
(2) Least Functionality Prevent Program Execution	73
(5) Least Functionality Authorized Software — Allow-by-Exception	74
CM-8 System Component Inventory	74
(1) System Component Inventory Updates During Installation and Removal	75
(3) System Component Inventory Automated Unauthorized Component Detection	76
CM-9 Configuration Management Plan	76
CM-10 Software Usage Restrictions	77
CM-11 User-Installed Software	78
CM-12 Information Location	78
(1) Information Location Automated Tools to Support Information Location	79
CONTINGENCY PLANNING (CP)	80
CP-1 Policy and Procedures	80
CP-2 Contingency Plan	81
(1) Contingency Plan Coordinate with Related Plans	82
(3) Contingency Plan Resume Mission and Business Functions	82
(8) Contingency Plan Identify Critical Assets	82
CP-3 Contingency Training	83
CP-4 Contingency Plan Testing	84
(1) Contingency Plan Testing Coordinate with Related Plans	84
CP-6 Alternate Storage Site	84
(1) Alternate Storage Site Separation from Primary Site	85
(3) Alternate Storage Site Accessibility	85
CP-7 Alternate Processing Site	86
(1) Alternate Processing Site Separation from Primary Site	86
(2) Alternate Processing Site Accessibility	87
(3) Alternate Processing Site Priority of Service	87
CP-8 Telecommunications Services	87
(1) Telecommunications Services Priority of Service Provisions	88
(2) Telecommunications Services Single Points of Failure	88
CP-9 System Backup	89
(1) System Backup Testing for Reliability and Integrity	89

(8) System Backup Cryptographic Protection	90
CP-10 System Recovery and Reconstitution	90
(2) System Recovery and Reconstitution Transaction Recovery	90
IDENTIFICATION AND AUTHENTICATION (IA)	92
IA-0 Use of Originating Agency Identifiers in Transactions and Information Exchanges ...	92
IA-1 Policy and Procedures	92
IA-2 Identification and Authentication (Organizational Users)	93
(1) Identification and Authentication (Organizational Users) Multi-Factor Authentication to Privileged Accounts	94
(2) Identification and Authentication (Organizational Users) Multi-Factor Authentication to Non-Privileged Accounts	94
(8) Identification and Authentication (Organizational Users) Access to Accounts — Replay Resistant.....	95
(12) Identification and Authentication (Organizational Users) Acceptance of PIV Credentials	95
IA-3 Device Identification and Authentication.....	95
IA-4 Identifier Management	96
(4) Identifier Management Identify User Status	97
IA-5 Authenticator Management	97
(1) Authenticator Management Authenticator Types	118
(a) Memorized Secret Authenticators and Verifiers:	118
(b) Look-Up Secret Authenticators and Verifiers	123
(c) Out-of-Band Authenticators and Verifiers	125
(d) OTP Authenticators and Verifiers	130
(e) Cryptographic Authenticators and Verifiers (Including Single- and Multi-Factor Cryptographic Authenticators, Both Hardware- and Software-Based)	134
(2) Authenticator Management Public Key Based Authentication.....	137
(6) Authenticator Management Protection of Authenticators	138
IA-6 Authentication Feedback	138
IA-7 Cryptographic Module Authenticationf.....	139
IA-8 Identification and Authentication (Non-Organizational Users)	139
(1) Identification and Authentication (Non-Organizational Users) Acceptance of PIV Credentials from Other Agencies.....	140
(2) Identification and Authentication (Non-Organizational Users) Acceptance of External Authenticators	140
(4) Identification and Authentication (Non-Organizational Users) Use of Defined Profiles	140
IA-11 Re-Authentication	141
IA-12 Identity Proofing.....	141
(2) Identity Proofing Identity Evidence	141
(3) Identity Proofing Identity Evidence Validation and Verification	142
(5) Identity Proofing Address Confirmation	164
INCIDENT RESPONSE (IR)	167
IR-1 Policy and Procedures.....	167
IR-2 Incident Response Training	168
(3) Incident Response Training Breach.....	168

IR-3 Incident Response Testing	169
(2) Incident Response Testing Coordination with Related Plans	169
IR-4 Incident Handling	169
(1) Incident Handling Automated Incident Handling Processes	170
IR-5 Incident Monitoring	170
IR-6 Incident Reporting	171
(1) Incident Reporting Automated Reporting	171
(3) Incident Reporting Supply Chain Coordination	171
IR-7 Incident Response Assistance	172
(1) Incident Response Assistance Automation Support for Availability of Information and Supportf	172
IR-8 Incident Response Plan	172
(1) Incident Response Plan Breaches	173
MAINTENANCE (MA)	175
MA-1 Policy and Procedures	175
MA-2 Controlled Maintenance	176
MA-3 Maintenance Tools	176
(1) Maintenance Tools Inspect Tools	177
(2) Maintenance Tools Inspect Media	177
(3) Maintenance Tools Prevent Unauthorized Removal	177
MA-4 Nonlocal Maintenance	178
MA-5 Maintenance Personnel	178
MA-6 Timely Maintenance	179
MEDIA PROTECTION (MP)	180
MP-1 Policy and Procedures	180
MP-2 Media Access	181
MP-3 Media Marking	181
MP-4 Media Storage	182
MP-5 Media Transport	183
MP-6 Media Sanitization	183
MP-7 Media Use	184
PHYSICAL AND ENVIRONMENTAL PROTECTION (PE)	186
PE-1 Policy and Procedures	186
PE-2 Physical Access Authorizations	187
PE-3 Physical Access Control	187
PE-4 Access Control for Transmission	188
PE-5 Access Control for Output Devices	188
PE-6 Monitoring Physical Access	189
(1) Monitoring Physical Access Intrusion Alarms and Surveillance Equipment	189
PE-8 Visitor Access Records	190
(3) Visitor Access Records Limit Personally Identifiable Information Elements	190
PE-9 Power Equipment and Cabling	190
PE-10 Emergency Shutoff	191
PE-11 Emergency Power	191
PE-12 Emergency Lighting	192
PE-13 Fire Protection	192

(1) Fire Protection Detection Systems — Automatic Activation and Notification	193
PE-14 Environmental Controls	193
PE-15 Water Damage Protection	193
PE-16 Delivery and Removal	194
PE-17 Alternate Work Site	194
PLANNING (PL).....	196
PL-1 Policy and Procedures.....	196
PL-2 System Security and Privacy Plans.....	197
PL-4 Rules of Behavior.....	199
(1) Rules of Behavior Social Media and External Site/Application Usage Restrictions	
199	
PL-8 Security and Privacy Architectures.....	200
PL-9 Central Management.....	201
PL-10 Baseline Selection.....	202
PL-11 Baseline Tailoring.....	202
PERSONNEL SECURITY (PS).....	204
PS-1 Policy and Procedures.....	204
PS-2 Position Risk Designation	205
PS-3 Personnel Screening.....	205
PS-4 Personnel Termination	207
PS-5 Personnel Transfer	208
PS-6 Access Agreements	209
PS-7 External Personnel Security	209
PS-8 Personnel Sanctions	210
PS-9 Position Descriptions	210
RISK ASSESSMENT (RA).....	213
RA-1 Policy and Procedures.....	213
RA-2 Security Categorization.....	214
RA-3 Risk Assessment.....	214
RA-5 Vulnerability Monitoring and Scanning.....	215
(2) Vulnerability Monitoring and Scanning Update Vulnerabilities to Be Scanned.....	217
(5) Vulnerability Monitoring and Scanning Privileged Access	217
(11) Vulnerability Monitoring and Scanning Public Disclosure Program.....	217
RA-7 Risk Response	218
RA-9 Criticality Analysis.....	218
SYSTEM AND SERVICES ACQUISITION (SA).....	220
SA-1 Policy and Procedures	220
SA-2 Allocation of Resources.....	221
SA-3 System Development Life Cycle	221
SA-4 Acquisition Process	222
(1) Acquisition Process Functional Properties of Controls	223
(2) Acquisition Process Design and Implementation Information for Controls	224
(9) Acquisition Process Functions, Ports, Protocols, and Services In Use.....	224
(10) Acquisition Process Use of Approved Piv Products.....	225
SA-5 System Documentation.....	225
SA-8 Security and Privacy Engineering Principles.....	226

(33) Security and Privacy Engineering Principles Minimization	227
SA-9 External System Services.....	227
(2) External System Services Identification of Functions, Ports, Protocols, and Services 230	
SA-10 Developer Configuration Management	230
SA-11 Developer Testing and Evaluation	231
SA-15 Development Process, Standards, and Tools.....	232
(1) Development Process, Standards, and Tools Criticality Analysis	233
SA-22 Unsupported System Components	234
SYSTEMS AND COMMUNICATIONS PROTECTION (SC)	235
SC-1 Policy and Procedures.....	235
SC-2 Separation of System and User Functionality.....	236
SC-4 Information in Shared System Resources	236
SC-5 Denial-of-Service Protection	237
SC-7 Boundary Protection	237
(3) Boundary Protection Access Points.....	238
(4) Boundary Protection External Telecommunications Services	238
(5) Boundary Protection Deny by Default — Allow by Exception	239
(7) Boundary Protection Split Tunneling for Remote Devices	239
(8) Boundary Protection Route Traffic to Authenticated Proxy Servers	240
(24) Boundary Protection Personally Identifiable Information	240
SC-8 Transmission Confidentiality and Integrity	240
(1) Transmission Confidentiality and Integrity Cryptographic Protection	241
SC-10 Network Disconnect	242
SC-12 Cryptographic Key Establishment and Management	242
SC-13 Cryptographic Protection.....	243
SC-15 Collaborative Computing Devices and Applications	243
SC-17 Public Key Infrastructure Certificates	244
SC-18 Mobile Code	244
SC-20 Secure Name/Address Resolution Service (Authoritative Source)	245
SC-21 Secure Name/Address Resolution Service (Recursive or Caching Resolver).....	245
SC-22 Architecture and Provisioning for Name/Address Resolution Service	246
SC-23 Session Authenticity	246
SC-28 Protection of Information at Rest	246
(1) Protection of Information at Rest Cryptographic Protection.....	247
SC-39 Process Isolation	248
SYSTEM AND INFORMATIONINTEGRITY (SI)	250
SI-1 Policy and Procedures.....	250
SI-2 Flaw Remediation	251
(2) Flaw Remediation Automated Flaw Remediation Status.....	252
SI-3 Malicious Code Protection.....	252
SI-4 System Monitoring.....	253
(2) System Monitoring Automated Tools and Mechanisms for Real-Time Analysis....	255
(4) System Monitoring Inbound and Outbound Communications Traffic.....	255
(5) System Monitoring System-Generated Alerts	255
SI-5 Security Alerts, Advisories, and Directives	256

SI-7 Software, Firmware, and Information Integrity	256
(1) Software, Firmware, and Information Integrity Integrity Checks	257
(7) Software, Firmware, and Information Integrity Integration of Detection and Response 257	
SI-8 Spam Protection	258
(2) Spam Protection Automatic Updates	258
SI-10 Information Input Validation	258
SI-11 Error Handling	259
SI-12 Information Management and Retention	259
(1) Information Management and Retention Limit Personally Identifiable Information Elements	260
(2) Information Management and Retention Minimize Personally Identifiable Information in Testing, Training, and Research	260
(3) Information Management and Retention Information Disposal	260
SI-16 Memory Protection	261
SUPPLY CHAIN RISK MANAGEMENT (SR)	262
SR-1 Policy and Procedures	262
SR-2 Supply Chain Risk Management Plan	263
(1) Supply Chain Risk Management Plan Establish SCRM Team	264
SR-5 Acquisition Strategies, Tools, and Methods	264
SR-8 Notification Agreements	265
SR-10 Inspection of Systems or Components	265
SR-12 Component Disposal	266
5.20 Policy Area 20: Mobile Devices	267
5.20.1 Wireless Communications Technologies	267
5.20.1.1 802.11 Wireless Protocols	267
5.20.1.2 Cellular Devices	268
5.20.1.2.1 Cellular Service Abroad	269
5.20.1.2.2 Voice Transmissions Over Cellular Devices	269
5.20.1.3 Bluetooth	269
5.20.1.4 Mobile Hotspots	269
5.20.2 Mobile Device Management (MDM)	270
5.20.3 Wireless Device Risk Mitigations	270
5.20.4 System Integrity	271
5.20.4.1 Patching/Updates	271
5.20.4.2 Malicious Code Protection	271
5.20.4.3 Personal Firewall	271
5.20.5 Incident Response	272
5.20.6 Access Control	272
5.20.7 Identification and Authentication	272
5.20.7.1 Local Device Authentication	272
5.20.7.2 Advanced Authentication	273
5.20.7.2.1 Compensating Controls	273
5.20.7.3 Device Certificates	273
Appendices	274
APPENDIX A: TERMS AND DEFINITIONS	A-1

APPENDIX B: ACRONYMS	B-1
APPENDIX C: NETWORK TOPOLOGY DIAGRAMS	C-1
APPENDIX D: SAMPLE INFORMATION EXCHANGE AGREEMENTS	D-1
D.1 CJIS User Agreement.....	D.1-1
D.2 Management Control Agreement.....	D.2-1
D.3 Noncriminal Justice Agency Agreement & Memorandum of Understanding.....	D.3-1
D.4 Interagency Connection Agreement.....	D.4-1
APPENDIX E: SECURITY FORUMS AND ORGANIZATIONAL ENTITIES	E-1
APPENDIX F: SAMPLE FORMS	F-1
F.1 Security Incident Response form.....	F.1-1
APPENDIX G: BEST PRACTICES	G-1
G.1 Virtualization	G.1-1
G.2 Voice over Internet Protocol	G.2-1
G.3 Cloud Computing.....	G.3-1
G.4 Mobile Appendix	G.4-1
G.5 Administrator Accounts for Least Privilege and Separation of Duties.....	G.5-1
G.6 Encryption.....	G.6-1
G.7 Incident Response	G.7-1
G.8 Secure Coding.....	G.8-1
APPENDIX H: SECURITY ADDENDUM.....	H-1
APPENDIX I: REFERENCES	I-1

LIST OF FIGURES

Figure 1 – Overview Diagram of Strategic Functions and Policy Components	4
Figure 2 – Dissemination of restricted and non-restricted NCIC data.....	13
Figure 3 – Information Exchange Agreements Implemented by a Local Police Department	15
Figure 4 – Security Awareness Training Use Cases	43
Figure 5 – A Local Police Department’s Configuration Management Controls	79
Figure 6 – Digital Identity Model	103
Figure 7 – Notional Strengths of Evidence Types	153
Figure 8 – Types of Identity Evidence Security Features	156
Figure 9 – Validating Identity Evidence	157
Figure 10 – Verification Methods and Strengths	159
Figure 11 – Incident Response Process Initiated by an Incident in a Local Police Department .	174
Figure 12 – A Local Police Department’s Media Management Policies.....	185
Figure 13 – Personnel Security Use Cases	211
Figure 14 – System and Communications Protection and Information Integrity Use Cases.....	248

LIST OF PRIORITIES

NOTE: An asterisk (“*”) in the Priority column indicates an existing control from version 5.9.

No.	Control Name	Enhancements	Priority
AC-1	POLICY AND PROCEDURES	AC-1	P2
AC-2	ACCOUNT MANAGEMENT	AC-2 (1) (2) (3) (4) (5) (13)	P1
AC-3	ACCESS ENFORCEMENT	AC-3 (14)	P1*
AC-4	INFORMATION FLOW ENFORCEMENT	AC-4	P1*
AC-5	SEPARATION OF DUTIES	AC-5	P1*
AC-6	LEAST PRIVILEGE	AC-6 (1) (2) (5) (7) (9) (10)	P1*
AC-7	UNSUCCESSFUL LOGON ATTEMPTS	AC-7	P3*
AC-8	SYSTEM USE NOTIFICATION	AC-8	P2*
AC-11	DEVICE LOCK	AC-11 (1)	P4*
AC-12	SESSION TERMINATION	AC-12	P3
AC-14	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION	AC-14	P4
AC-17	REMOTE ACCESS	AC-17 (1) (2) (3) (4)	P1
AC-18	WIRELESS ACCESS	AC-18 (1) (3)	P2*
AC-19	ACCESS CONTROL FOR MOBILE DEVICES	AC-19 (5)	P2*
AC-20	USE OF EXTERNAL SYSTEMS	AC-20 (1) (2)	P1
AC-21	INFORMATION SHARING	AC-21	P3*
AC-22	PUBLICLY ACCESSIBLE CONTENT	AC-22	P4
AT-1	POLICY AND PROCEDURES	AT-1	P2
AT-2	LITERACY TRAINING AND AWARENESS	AT-2 (2) (3)	P2*
AT-3	ROLE-BASED TRAINING	AT-3	P2*
AT-3	ROLE-BASED TRAINING PROCESSING PERSONALLY IDENTIFIABLE INFORMATION	AT-3 (5)	P2
AT-4	TRAINING RECORDS	AT-4	P4*
AU-1	POLICY AND PROCEDURES	AU-1	P2
AU-2	EVENT LOGGING	AU-2	P2*
AU-3	CONTENT OF AUDIT RECORDS	AU-3 (1)	P2*
AU-3	CONTENT OF AUDIT RECORDS LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS	AU-3 (3)	P2
AU-4	AUDIT LOG STORAGE CAPACITY	AU-4	P2
AU-5	RESPONSE TO AUDIT LOGGING PROCESS FAILURES	AU-5	P2*
AU-6	AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING	AU-6 (1) (3)	P2*
AU-7	AUDIT RECORD REDUCTION AND REPORT GENERATION	AU-7 (1)	P3
AU-8	TIME STAMPS	AU-8	P2*
AU-9	PROTECTION OF AUDIT INFORMATION	AU-9 (4)	P2*
AU-11	AUDIT RECORD RETENTION	AU-11	P4*
AU-12	AUDIT RECORD GENERATION	AU-12	P2
CA-1	POLICY AND PROCEDURES	CA-1	P2
CA-2	CONTROL ASSESSMENTS	CA-2 (1)	P3
CA-3	INFORMATION EXCHANGE	CA-3	P2*
CA-5	PLAN OF ACTION AND MILESTONES	CA-5	P4

No.	Control Name	Enhancements	Priority
CA-6	AUTHORIZATION	CA-6	P3
CA-7	CONTINUOUS MONITORING	CA-7 (1) (4)	P1
CA-9	INTERNAL SYSTEM CONNECTIONS	CA-9	P3
CM-1	POLICY AND PROCEDURES	CM-1	P2
CM-2	BASELINE CONFIGURATION	CM-2 (2) (3) (7)	P1
CM-3	CONFIGURATION CHANGE CONTROL	CM-3 (2) (4)	P2
CM-4	IMPACT ANALYSES	CM-4 (2)	P3
CM-5	ACCESS RESTRICTIONS FOR CHANGE	CM-5	P1
CM-6	CONFIGURATION SETTINGS	CM-6	P1
CM-7	LEAST FUNCTIONALITY	CM-7 (1) (2) (5)	P1
CM-8	SYSTEM COMPONENT INVENTORY	CM-8 (1) (3)	P1
CM-9	CONFIGURATION MANAGEMENT PLAN	CM-9	P2
CM-10	SOFTWARE USAGE RESTRICTIONS	CM-10	P3
CM-11	USER-INSTALLED SOFTWARE	CM-11	P2
CM-12	INFORMATION LOCATION	CM-12 (1)	P2
CP-1	POLICY AND PROCEDURES	CP-1	P2
CP-2	CONTINGENCY PLAN	CP-2 (1) (3) (8)	P2
CP-3	CONTINGENCY TRAINING	CP-3	P3
CP-4	CONTINGENCY PLAN TESTING	CP-4 (1)	P3
CP-6	ALTERNATE STORAGE SITE	CP-6 (1) (3)	P2
CP-7	ALTERNATE PROCESSING SITE	CP-7 (1) (2) (3)	P2
CP-8	TELECOMMUNICATIONS SERVICES	CP-8 (1) (2)	P2
CP-9	SYSTEM BACKUP	CP-9 (1) (8)	P2
CP-10	SYSTEM RECOVERY AND RECONSTITUTION	CP-10 (2)	P2
IA-1	POLICY AND PROCEDURES	IA-1	P2
IA-2	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)	IA-2 (1) (2) (8) (12)	P1
IA-3	DEVICE IDENTIFICATION AND AUTHENTICATION	IA-3	P2
IA-4	IDENTIFIER MANAGEMENT	IA-4 (4)	P2*
IA-5	AUTHENTICATOR MANAGEMENT	IA-5 (1) (2) (6)	P1
IA-6	AUTHENTICATION FEEDBACK	IA-6	P3*
IA-7	CRYPTOGRAPHIC MODULE AUTHENTICATION	IA-7	P2
IA-8	IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)	IA-8 (1) (2) (4)	P2
IA-11	RE-AUTHENTICATION	IA-11	P2
IA-12	IDENTITY PROOFING	IA-12 (2) (3) (5)	P2
IR-1	POLICY AND PROCEDURES	IR-1	P2*
IR-2	INCIDENT RESPONSE TRAINING	IR-2	P3*
IR-2	INCIDENT RESPONSE TRAINING BREACH	IR-2 (3)	P3
IR-3	INCIDENT RESPONSE TESTING	IR-3 (2)	P3
IR-4	INCIDENT HANDLING	IR-4 (1)	P2*
IR-5	INCIDENT MONITORING	IR-5	P2*
IR-6	INCIDENT REPORTING	IR-6 (1) (3)	P2*
IR-7	INCIDENT RESPONSE ASSISTANCE	IR-7 (1)	P3*

No.	Control Name	Enhancements	Priority
IR-8	INCIDENT RESPONSE PLAN	IR-8	P2*
IR-8	INCIDENT RESPONSE PLAN BREACHES	IR-8 (1)	P2
MA-1	POLICY AND PROCEDURES	MA-1	P2
MA-2	CONTROLLED MAINTENANCE	MA-2	P3
MA-3	MAINTENANCE TOOLS	MA-3 (1) (2) (3)	P4
MA-4	NONLOCAL MAINTENANCE	MA-4	P3
MA-5	MAINTENANCE PERSONNEL	MA-5	P3
MA-6	TIMELY MAINTENANCE	MA-6	P3
MP-1	POLICY AND PROCEDURES	MP-1	P2*
MP-2	MEDIA ACCESS	MP-2	P2*
MP-3	MEDIA MARKING	MP-3	P3*
MP-4	MEDIA STORAGE	MP-4	P2*
MP-5	MEDIA TRANSPORT	MP-5	P2*
MP-6	MEDIA SANITIZATION	MP-6	P2*
MP-7	MEDIA USE	MP-7	P2*
PE-1	POLICY AND PROCEDURES	PE-1	P2
PE-2	PHYSICAL ACCESS AUTHORIZATIONS	PE-2	P2*
PE-3	PHYSICAL ACCESS CONTROL	PE-3	P2*
PE-4	ACCESS CONTROL FOR TRANSMISSION	PE-4	P2*
PE-5	ACCESS CONTROL FOR OUTPUT DEVICES	PE-5	P3*
PE-6	MONITORING PHYSICAL ACCESS	PE-6 (1)	P2*
PE-8	VISITOR ACCESS RECORDS	PE-8 (3)	P4
PE-9	POWER EQUIPMENT AND CABLING	PE-9	P2
PE-10	EMERGENCY SHUTOFF	PE-10	P2
PE-11	EMERGENCY POWER	PE-11	P2
PE-12	EMERGENCY LIGHTING	PE-12	P2
PE-13	FIRE PROTECTION	PE-13 (1)	P2
PE-14	ENVIRONMENTAL CONTROLS	PE-14	P2
PE-15	WATER DAMAGE PROTECTION	PE-15	P2
PE-16	DELIVERY AND REMOVAL	PE-16	P3
PE-17	ALTERNATE WORK SITE	PE-17	P3*
PL-1	POLICY AND PROCEDURES	PL-1	P2
PL-2	SYSTEM SECURITY AND PRIVACY PLANS	PL-2	P2
PL-4	RULES OF BEHAVIOR	PL-4 (1)	P3
PL-8	SECURITY AND PRIVACY ARCHITECTURES	PL-8	P2
PL-9	CENTRAL MANAGEMENT	PL-9	P4
PL-10	BASELINE SELECTION	PL-10	P3
PL-11	BASELINE TAILORING	PL-11	P3
PS-1	POLICY AND PROCEDURES	PS-1	P2
PS-2	POSITION RISK DESIGNATION	PS-2	P2
PS-3	PERSONNEL SCREENING	PS-3	P2*
PS-4	PERSONNEL TERMINATION	PS-4	P2

No.	Control Name	Enhancements	Priority
PS-5	PERSONNEL TRANSFER	PS-5	P3*
PS-6	ACCESS AGREEMENTS	PS-6	P4
PS-7	EXTERNAL PERSONNEL SECURITY	PS-7	P2*
PS-8	PERSONNEL SANCTIONS	PS-8	P4
PS-9	POSITION DESCRIPTIONS	PS-9	P4
RA-1	POLICY AND PROCEDURES	RA-1	P2
RA-2	SECURITY CATEGORIZATION	RA-2	P2
RA-3	RISK ASSESSMENT	RA-3 (1)	P2
RA-5	VULNERABILITY MONITORING AND SCANNING	RA-5 (2) (5) (11)	P1
RA-7	RISK RESPONSE	RA-7	P2
RA-9	CRITICALITY ANALYSIS	RA-9	P2
SA-1	POLICY AND PROCEDURES	SA-1	P2
SA-2	ALLOCATION OF RESOURCES	SA-2	P2
SA-3	SYSTEM DEVELOPMENT LIFE CYCLE	SA-3	P2
SA-4	ACQUISITION PROCESS	SA-4 (1) (2) (9) (10)	P2
SA-5	SYSTEM DOCUMENTATION	SA-5	P3
SA-8	SECURITY AND PRIVACY ENGINEERING PRINCIPLES	SA-8 (33)	P2
SA-9	EXTERNAL SYSTEM SERVICES	SA-9 (2)	P2
SA-10	DEVELOPER CONFIGURATION MANAGEMENT	SA-10	P2
SA-11	DEVELOPER TESTING AND EVALUATION	SA-11	P2
SA-15	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS	SA-15 (3)	P3
SA-22	UNSUPPORTED SYSTEM COMPONENTS	SA-22	P2
SC-1	POLICY AND PROCEDURES	SC-1	P2
SC-2	SEPARATION OF SYSTEM AND USER FUNCTIONALITY	SC-2	P2*
SC-4	INFORMATION IN SHARED SYSTEM RESOURCES	SC-4	P2*
SC-5	DENIAL-OF-SERVICE PROTECTION	SC-5	P2
SC-7	BOUNDARY PROTECTION	SC-7 (3) (4) (5) (7) (8) (24)	P1
SC-8	TRANSMISSION CONFIDENTIALITY AND INTEGRITY	SC-8 (1)	P2*
SC-10	NETWORK DISCONNECT	SC-10	P3
SC-12	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	SC-12	P2*
SC-13	CRYPTOGRAPHIC PROTECTION	SC-13	P2*
SC-15	COLLABORATIVE COMPUTING DEVICES AND APPLICATIONS	SC-15	P2
SC-17	PUBLIC KEY INFRASTRUCTURE CERTIFICATES	SC-17	P2*
SC-18	MOBILE CODE	SC-18	P3
SC-20	SECURE NAME/ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)	SC-20	P2
SC-21	SECURE NAME/ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)	SC-21	P2
SC-22	ARCHITECTURE AND PROVISIONING FOR NAME/ADDRESS RESOLUTION SERVICE	SC-22	P2
SC-23	SESSION AUTHENTICITY	SC-23	P2
SC-28	PROTECTION OF INFORMATION AT REST	SC-28 (1)	P2*
SC-39	PROCESS ISOLATION	SC-39	P2*
SI-1	POLICY AND PROCEDURES	SI-1	P2
SI-2	FLAW REMEDIATION	SI-2 (2)	P1

No.	Control Name	Enhancements	Priority
SI-3	MALICIOUS CODE PROTECTION	SI-3	P1
SI-4	SYSTEM MONITORING	SI-4 (2) (4) (5)	P1
SI-5	SECURITY ALERTS, ADVISORIES, AND DIRECTIVES	SI-5	P2*
SI-7	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY	SI-7 (1) (7)	P1
SI-8	SPAM PROTECTION	SI-8 (2)	P3*
SI-10	INFORMATION INPUT VALIDATION	SI-10	P1
SI-11	ERROR HANDLING	SI-11	P3
SI-12	INFORMATION MANAGEMENT AND RETENTION	SI-12 (1) (2) (3)	P3
SI-16	MEMORY PROTECTION	SI-16	P2
SI-18	PERSONALLY IDENTIFIABLE INFORMATION QUALITY OPERATIONS	SI-18 (4)	P4
SI-19	DE-IDENTIFICATION	SI-19	P4
SR-1	POLICY AND PROCEDURES	SR-1	P2
SR-2	SUPPLY CHAIN RISK MANAGEMENT PLAN	SR-2 (1)	P3
SR-3	SUPPLY CHAIN CONTROLS AND PROCESSES	SR-3	P3
SR-5	ACQUISITION STRATEGIES, TOOLS, AND METHODS	SR-5	P2
SR-6	SUPPLIER ASSESSMENTS AND REVIEWS	SR-6	P2
SR-8	NOTIFICATION AGREEMENTS	SR-8	P3
SR-10	INSPECTION OF SYSTEMS OR COMPONENTS	SR-10	P3
SR-11	COMPONENT AUTHENTICITY	SR-11 (1) (2)	P2
SR-12	COMPONENT DISPOSAL	SR-12	P3

1 INTRODUCTION

This section details the purpose of this document, its scope, relationship to other information security policies, and its distribution constraints.

1.1 Purpose

The CJISSECPOL provides Criminal Justice Agencies (CJA), Noncriminal Justice Agencies (NCJA), and Interface Agencies (IA) with a minimum set of security requirements for access to Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division systems and information and to protect and safeguard Criminal Justice Information (CJI). The essential premise of the CJISSECPOL is to provide the appropriate controls to ensure the continuity of the protection of CJI, from creation through dissemination or destruction, whether at rest or in transit.

1.2 Scope

At the consent of the advisory process, and taking into consideration federal law and state statutes, the CJISSECPOL applies to all entities with access to, or that operate systems which are used to process, store, or transmit CJI. The CJISSECPOL provides minimum security requirements associated with the creation, viewing, modification, transmission, dissemination, storage, or destruction of CJI.

Entities engaged in the interstate exchange of CHRI for noncriminal justice purposes are also governed by the standards and rules promulgated by the Compact Council.

1.3 Relationship to Local Security Policy and Other Policies

The CJISSECPOL may be used as the sole security policy for the agency. The local agency may complement the CJISSECPOL with a local policy, or the agency may develop their own stand-alone security policy; however, the CJISSECPOL shall always be the minimum standard. State, local, Tribal, territorial (SLTT), and Federal agencies may augment or implement more stringent policies or requirements.

The agency shall develop, disseminate, and maintain formal, documented policy and procedures to facilitate the implementation of the CJISSECPOL and, where applicable, the local security policy. The policies and procedures shall be consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidance. Procedures developed for CJISSECPOL areas can be developed for the security program in general, and for a particular information system, when required.

1.4 Terminology Used in This Document

Effective in version 5.9.5, priority and implementation markings have been added to the modernized controls. Based on the FBI Director approved APB recommendation, beginning October 1, 2024, requirements existing prior to the CJISSECPOL modernization (i.e., version 5.9) and those identified as Priority 1 ([Priority 1]) will be the set of sanctionable requirements.

- Non-modernized sections do not have markings but are considered “existing” requirements and continue to be auditable and sanctionable.

- “Existing” modernized requirements and indicated by the [Existing] marking.
- Priority 1 modernized requirements are indicated by the [Priority 1] marking.
- All [Priority 2], [Priority 3], and [Priority 4] modernized requirements fall into a zero-cycle status. The zero-cycle begins October 1, 2024 and ends September 30, 2027.

The following terms are used interchangeably throughout this document:

- **Agency and Organization:** The two terms in this document refer to any entity that submits or receives information, by any means, to/from FBI CJIS systems or services.
- **Organizational Personnel:** Individuals belonging to an agency or organization (see above) or contracted to an agency or organization to provide services under contract.
- **Information and Data:** Both terms refer to CJI.
- **System, Information System, Service, or named applications like NCIC:** all refer to connections to the FBI’s criminal justice information repositories and the equipment used to establish said connections.
- **Requirement and Control:** These terms refer to a condition or capability that must be met or possessed by a system or system element to satisfy an agreement, standard, specification, or other formally imposed document.

Appendix A and B provide extensive lists of the terms and acronyms.

Appendix I contains all of the references used in this Policy and may contain additional sources that could apply to any section.

1.5 Distribution of the CJIS Security Policy

The CJISSECPOL, version 6.0 and later, is a publicly available document and may be posted and shared without restrictions.

2 CJIS SECURITY POLICY APPROACH

The CJISSECPOL represents the shared responsibility among FBI CJIS, CJIS Systems Agency (CSA), State Identification Bureaus (SIB), and Interface Agency (IA) for the appropriate protection of CJI.

2.1 CJIS Security Policy Vision Statement

The executive summary of this document describes the vision in terms of business needs for confidentiality, integrity, and availability of information. The APB collaborates with the FBI CJIS Division to ensure that the Policy remains updated to meet evolving business, technology and security needs.

2.2 Architecture Independent

The CJISSECPOL looks at the data (information), services, and protection controls that apply regardless of the implementation architecture. Architectural independence is not intended to lessen the importance of systems, but provide for the replacement of one technology with another while ensuring the controls required to protect the information remain constant. This objective and conceptual focus on security policy areas provide the guidance and standards while avoiding the impact of the constantly changing landscape of technical innovations. The architectural independence of the Policy provides agencies with the flexibility for tuning their information security infrastructure and policies to reflect their own environments.

2.3 Risk Versus Realism

Each agency faces risk unique to that agency. It is quite possible that several agencies could encounter the same type of risk however depending on resources would mitigate that risk differently. In that light, a risk-based approach can be used when implementing requirements.

3 ROLES AND RESPONSIBILITIES

3.1 Shared Management Philosophy

In the scope of information security, the FBI CJIS Division employs a shared management philosophy with SLTT and Federal criminal justice agencies. Although an advisory policy board for the NCIC has existed since 1969, the Director of the FBI established the CJIS APB in March 1994 to enable appropriate input and recommend policy with respect to CJIS services. Through the APB and its Subcommittees and Working Groups, consideration is given to the needs of the criminal justice and law enforcement community regarding public policy, statutory and privacy aspects, as well as national security relative to CJIS systems and information. The APB, including a representative of the Compact Council, represents criminal and noncriminal justice agencies throughout the United States, its territories, and Canada.

The FBI has a similar relationship with the Compact Council, which governs the interstate exchange of criminal history records for noncriminal justice purposes. The Compact Council is mandated by federal law to promulgate rules and procedures for the use of the Interstate Identification Index (III) for noncriminal justice purposes. To meet that responsibility, the Compact Council depends on the CJISSECPOL as the definitive source for standards defining the security and privacy of records exchanged with noncriminal justice practitioners.

3.2 Roles and Responsibilities for Agencies and Parties

It is the responsibility of all agencies covered under this Policy to ensure the protection of CJI between the FBI CJIS Division and its user community. The following figure provides an abstract representation of the strategic functions and roles such as governance and operations.

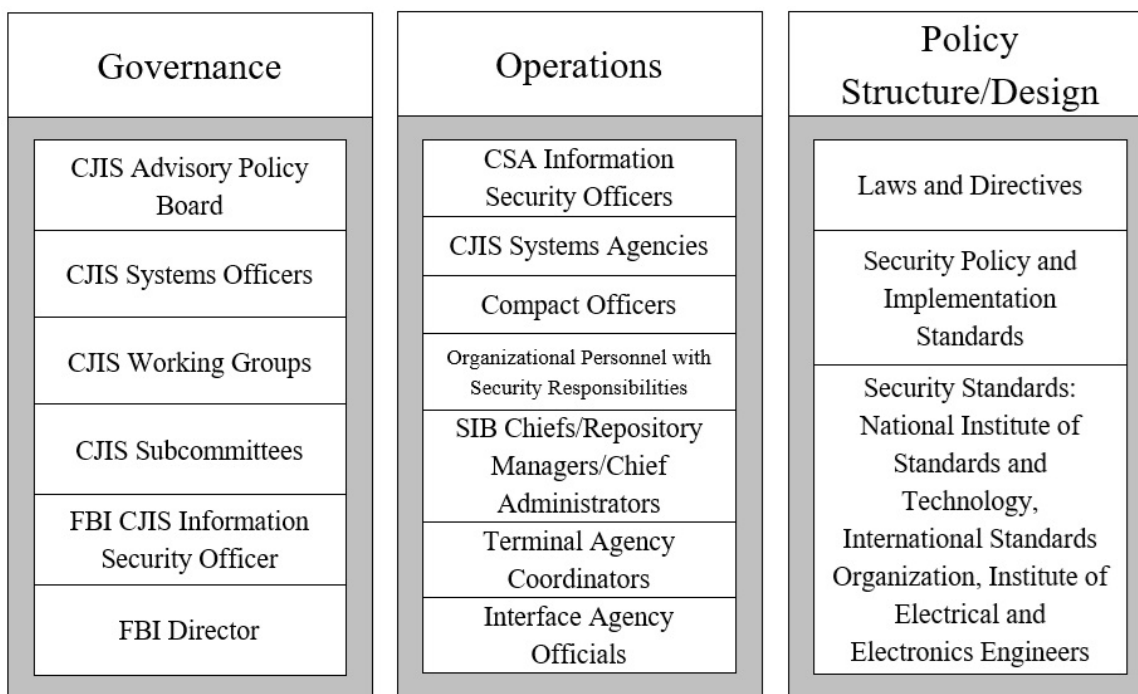


Figure 1 – Overview Diagram of Strategic Functions and Policy Components

This section provides a description of the following entities and roles:

1. CJIS Systems Agency (CSA).
2. CJIS Systems Officer (CSO).
3. Terminal Agency Coordinator (TAC).
4. Criminal Justice Agency (CJA).
5. Noncriminal Justice Agency (NCJA).
6. Contracting Agency (CA).
7. Agency Coordinator (AC).
8. CJIS Systems Agency (CSA) Information Security Officer (ISO).
9. Organizational Personnel with Security Responsibilities.
10. FBI CJIS Division Information Security Officer (ISO).
11. SIB Chief/Repository Manager/Chief Administrator.
12. Interface Agency (IA) Official
13. State Compact Officer (SCO).

3.2.1 CJIS Systems Agencies (CSA)

The CSA is responsible for establishing and administering an information technology security program throughout the CSA's user community, to include the local levels. The head of each CSA shall appoint a CJIS Systems Officer (CSO). The CSA may impose more stringent or additional protection measures than outlined in this document. Such decisions shall be documented and kept current.

3.2.2 CJIS Systems Officer (CSO)

The CSO is an individual located within the CSA responsible for the administration of the CJIS network for the CSA. Pursuant to the Bylaws for the CJIS Advisory Policy Board and Working Groups, the role of CSO shall not be outsourced. The CSO may delegate responsibilities to subordinate agencies. The CSO shall set, maintain, and enforce the following:

1. Standards for the selection, supervision, and separation of personnel who have access to CJI.
2. Policy governing the operation of computers, access devices, circuits, hubs, routers, firewalls, and other components that comprise and support a telecommunications network and related CJIS systems used to process, store, or transmit CJI, guaranteeing the priority of service required by the law enforcement community, confidentiality, integrity, and availability of CJI.
 - a. Ensure appropriate use, enforce system discipline, and ensure CJIS Division operating procedures are followed by all users of the respective services and information.
 - b. Ensure state/federal agency compliance with policies approved by the APB and adopted by the FBI.

- c. Ensure the appointment of the CSA ISO and determine the extent of authority to the CSA ISO.
- d. Ensure the designation of a Terminal Agency Coordinator (TAC) within each agency with devices accessing CJIS systems.
- e. Ensure each agency having access to CJI has someone designated as the Organizational Personnel with Security Responsibilities.
- f. Ensure each Organizational Personnel with Security Responsibilities receives enhanced security awareness training (ref. Awareness and Training (AT)).
- g. Approve access to FBI CJIS systems.
- h. Assume ultimate responsibility for managing the security of CJIS systems within their state and/or agency.
- i. Perform other related duties outlined by the user agreements with the FBI CJIS Division.

3. External System Services of Criminal Justice Functions

Responsibility for the management and control of security requirements for information systems which process, store, or transmit CJI shall remain with the CJA. Management and control includes the authority to:

- a. Set and enforce standards for the selection, supervision, and termination of access to CJI;
- b. Set and enforce policy governing the operation of computers, circuits, and telecommunications terminals,
- c. Guarantee the priority service as determined by the CSA.

3.2.3 Terminal Agency Coordinator (TAC)

The TAC serves as the point-of-contact at the local agency for matters relating to CJIS information access. The TAC administers CJIS systems programs within the local agency and oversees the agency's compliance with CJIS systems policies.

3.2.4 Criminal Justice Agency (CJA)

A CJA is defined as a court, a governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspectors General Offices are included.

3.2.5 Noncriminal Justice Agency (NCJA)

A NCJA is defined (for the purposes of access to CJI) as an entity or any subunit thereof that provides services primarily for purposes other than the administration of criminal justice.

3.2.6 Contracting Agency (CA)

A CA is an agency, whether a CJA, NCJA (public), or NCJA (private), that enters into an agreement with a private contractor subject to the CJIS Security Addendum, The Security and Management Control Outsourcing Standard for Non-Channelers, of the Security and Management Control Outsourcing Standard for Channeling. The CA entering into an agreement with a contractor shall appoint an Agency Coordinator.

3.2.7 Agency Coordinator (AC)

An AC is a staff member of the CGA who manages the agreement between the Contractor and agency. The AC shall be responsible for the supervision and integrity of the system, training and continuing education of employees and operators, scheduling of initial training and testing, and certification testing and all required reports by NCIC. The AC shall:

1. Understand the communications, records capabilities, and needs of the Contractor which is accessing federal and state records through or because of its relationship with the CGA.
2. Participate in related meetings and provide input and comments for system improvement.
3. Receive information from the CGA (e.g., system updates) and disseminate it to appropriate Contractor employees.
4. Maintain and update manuals applicable to the effectuation of the agreement, and provide them to the Contractor.
5. Maintain up-to-date records of Contractor's employees who access the system, including name, date of birth, social security number, date fingerprint card(s) submitted, date security clearance issued, and date initially trained, tested, certified or recertified (if applicable).
6. Train or ensure the training of Contractor personnel. If Contractor personnel access NCIC, schedule the operators for testing or a certification exam with the CSA staff, or AC staff with permission from the CSA staff as consistent with the NCIC policy.
7. The AC will not permit an untrained/untested or non-certified Contractor employee to access CJI or systems supporting CJI where access to CJI can be gained.
8. Where appropriate, ensure compliance by the Contractor with NCIC validation requirements.
9. Provide completed applicant fingerprint cards on each Contractor employee who accesses the system to the CGA (or, where appropriate, CSA) for criminal background investigation prior to such employee accessing the system.
10. Any other responsibility for the AC promulgated by the FBI.

3.2.8 CJIS Systems Agency Information Security Officer (CSA ISO)

The CSA ISO shall:

1. Serve as the security point of contact (POC) to the FBI CJIS Division ISO.
2. Document technical compliance with the CJIS Security Policy with the goal to assure the confidentiality, integrity, and availability of criminal justice information to the user community throughout the CSA's user community, to include the local level.

3. Document and provide assistance for implementing the security-related controls for the Interface Agency and its users.
4. Establish a security incident response and reporting procedure to discover, investigate, document, and report to the CSA, the affected criminal justice agency, and the FBI CJIS Division ISO major incidents that significantly endanger the security or integrity of CJI.

3.2.9 Organizational Personnel with Security Responsibilities

Each Organizational Personnel with Security Responsibilities shall:

1. Identify who is using the CSA approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
2. Identify and document how the equipment is connected to the state system.
3. Ensure that personnel security screening procedures are being followed as stated in this Policy.
4. Ensure the approved and appropriate security measures are in place and working as expected.
5. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.

3.2.10 FBI CJIS Division Information Security Officer (FBI CJIS ISO)

The FBI CJIS ISO shall:

1. Maintain the CJIS Security Policy.
2. Disseminate the FBI Director approved CJIS Security Policy.
3. Serve as a liaison with the CSA's ISO and with other personnel across the CJIS community and in this regard provide technical guidance as to the intent and implementation of operational and technical policy issues.
4. Serve as a point-of-contact (POC) for computer incident notification and distribution of security alerts to the CSOs and ISOs.
5. Assist with developing audit compliance guidelines as well as identifying and reconciling security-related issues.
6. Develop and participate in information security training programs for the CSOs and ISOs, and provide a means by which to acquire feedback to measure the effectiveness and success of such training.
7. Maintain a security policy resource center (SPRC) on FBI.gov and keep the CSOs and ISOs updated on pertinent information.

3.2.11 Repository Manager

The State Identification Bureau (SIB) Chief, i.e., Repository Manager or Chief Administrator, is the designated manager of the agency having oversight responsibility for a state's fingerprint identification services. If both state fingerprint identification services and CJIS systems control are managed within the same state agency, the SIB Chief and CSO may be the same person.

3.2.12 IA Official

The IA Official is an employee of the IA responsible for planning necessary hardware, software, funding, and training for the IA's authorized access to the CJIS Division's systems. The IA Official shall not be a contract employee.

3.2.13 State Compact Officer (SCO)

Pursuant to the National Crime Prevention and Privacy Compact, each party state shall appoint a Compact Officer who shall ensure that Compact provisions and rules, procedures, and standards established by the Compact Council are complied with in their respective state.

4 CRIMINAL JUSTICE INFORMATION AND PERSONALLY IDENTIFIABLE INFORMATION

4.1 Criminal Justice Information (CJI)

Criminal Justice Information is the term used to refer to all of the FBI CJIS provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data. The following categories of CJI describe the various data sets housed by the FBI CJIS architecture:

1. Biometric Data—data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population. Used to identify individuals, to include: fingerprints, palm prints, iris scans, and facial recognition data.
2. Identity History Data—textual data that corresponds with an individual’s biometric data, providing a history of criminal and/or civil events for the identified individual.
3. Biographic Data—information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case.
4. Property Data—information about vehicles and property associated with crime when accompanied by any personally identifiable information (PII).
5. Case/Incident History—information about the history of criminal incidents.

The following type of data are exempt from the protection levels required for CJI: transaction control type numbers (e.g., ORI, NIC, UCN, etc.) when not accompanied by information that reveals CJI or PII.

The intent of the CJIS Security Policy is to ensure the protection of the aforementioned CJI until the information is: released to the public via authorized dissemination (e.g., within a court system; presented in crime reports data; released in the interest of public safety); purged or destroyed in accordance with applicable record retention rules. CJI introduced into the court system pursuant to a judicial proceeding that can be released to the public via a public records request is not subject to the CJIS Security Policy.

4.1.1 Criminal History Record Information (CHRI)

Criminal History Record Information (CHRI), sometimes informally referred to as “restricted data”, is a subset of CJI. Due to its comparatively sensitive nature, additional controls are required for the access, use and dissemination of CHRI. In addition to the dissemination restrictions outlined below, Title 28, Part 20, Code of Federal Regulations (CFR), defines CHRI and provides the regulatory guidance for dissemination of CHRI. While the CJIS Security Policy attempts to be architecturally independent, the III and the NCIC are specifically identified in Title 28, Part 20, CFR, and the NCIC Operating Manual, as associated with CHRI.

4.2 Access, Use and Dissemination of Criminal History Record Information (CHRI), NCIC Restricted Files Information, and NCIC Non-Restricted Files Information

This section describes the requirements for the access, use and dissemination of CHRI, NCIC restricted files information, and NCIC non-restricted files information.

4.2.1 Proper Access, Use, and Dissemination of CHRI

Information obtained from the III is considered CHRI. Rules governing the access, use, and dissemination of CHRI are found in Title 28, Part 20, CFR. The III shall be accessed only for an authorized purpose. Further, CHRI shall only be used for an authorized purpose consistent with the purpose for which III was accessed. Dissemination to another agency is authorized if (a) the other agency is an Authorized Recipient of such information and is being serviced by the accessing agency, or (b) the other agency is performing personnel and appointment functions for criminal justice employment applicants.

4.2.2 Proper Access, Use, and Dissemination of NCIC Restricted Files Information

The NCIC hosts restricted files and non-restricted files. NCIC restricted files are distinguished from NCIC non-restricted files by the policies governing their access and use. Proper access to, use, and dissemination of data from restricted files shall be consistent with the access, use, and dissemination policies concerning the III described in Title 28, Part 20, CFR, and the NCIC Operating Manual. The restricted files, which shall be protected as CHRI, are as follows:

1. Gang Files
2. Threat Screening Center Files
3. Supervised Release Files
4. National Sex Offender Registry Files
5. Historical Protection Order Files of the NCIC
6. Identity Theft Files
7. Protective Interest Files
8. Person With Information (PWI) data in the Missing Person Files
9. Violent Person File
10. NICS Denied Transactions File

The remaining NCIC files are considered non-restricted files.

4.2.3 Proper Access, Use, and Dissemination of NCIC Non-Restricted Files Information

4.2.3.1 For Official Purposes

NCIC non-restricted files are those not listed as restricted files in Section 4.2.2. NCIC non-restricted files information may be accessed and used for any authorized purpose consistent with

the inquiring agency's responsibility. Information obtained may be disseminated to (a) other government agencies or (b) private entities authorized by law to receive such information for any purpose consistent with their responsibilities.

4.2.3.2 For Other Authorized Purposes

NCIC non-restricted files may be accessed for other purposes consistent with the resources of the inquiring agency; however, requests for bulk data are discouraged. Information derived from NCIC non-restricted files for other than law enforcement purposes can be used by authorized criminal justice personnel only to confirm the status of a person or property (i.e., wanted or stolen). An inquiring agency is authorized to charge a nominal administrative fee for such service. Non-restricted files information shall not be disseminated commercially.

A response to a NCIC person inquiry may include NCIC restricted files information as well as NCIC non-restricted files information. Agencies shall not disseminate restricted files information for purposes other than law enforcement.

4.2.3.3 CSO Authority in Other Circumstances

If no federal, state or local law or policy prohibition exists, the CSO may exercise discretion to approve or deny dissemination of NCIC non-restricted file information.

4.2.4 Storage

When CHRI is stored, agencies shall establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of the information. These records shall be stored for extended periods only when they are key elements for the integrity and/or utility of case files and/or criminal record files. See Section 5.9 for physical security controls.

4.2.5 Justification and Penalties

4.2.5.1 Justification

In addition to the use of purpose codes and logging information, all users shall provide a reason for all III inquiries whenever requested by NCIC System Managers, CSAs, local agency administrators, or their representatives.

4.2.5.2 Penalties

Improper access, use or dissemination of CHRI and NCIC Non-Restricted Files information is serious and may result in administrative sanctions including, but not limited to, termination of services and state and federal criminal penalties.

4.3 Personally Identifiable Information (PII)

For the purposes of this document, PII is information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. Any FBI CJIS provided data maintained by an agency, including but not limited to, education, financial transactions, medical history, and criminal or employment history may include PII. A criminal history record for

example inherently contains PII as would a Law Enforcement National Data Exchange (N-DEx) case file.

PII shall be extracted from CJI for the purpose of official business only. Agencies shall develop policies, based on state and local privacy rules, to ensure appropriate controls are applied when handling PII extracted from CJI. Due to the expansive nature of PII, this Policy does not specify auditing, logging, or personnel security requirements associated with the life cycle of PII.

Figure 2 – Dissemination of restricted and non-restricted NCIC data

A citizen of Springfield went to the Springfield Police Department to request whether his new neighbor, who had been acting suspiciously, had an outstanding warrant. The Springfield Police Department ran an NCIC persons inquiry, which produced a response that included a Wanted Person File (non-restricted file) record and a Threat Screening Center File (restricted file) record. The Springfield Police Department advised the citizen of the outstanding warrant but did not disclose any information concerning the subject being on the Threat Screening Center File.

5 POLICY AND IMPLEMENTATION

The policy areas focus upon the data and services that the FBI CJIS Division exchanges and provides to the criminal justice community and its partners. Each policy area provides both strategic reasoning and tactical implementation requirements and standards.

While the major theme of the policy areas is concerned with electronic exchange directly with the FBI, it is understood that further dissemination of CJI to Authorized Recipients by various means (hard copy, e-mail, web posting, etc.) constitutes a significant portion of CJI exchanges. Regardless of its form, use, or method of dissemination, CJI requires protection throughout its life.

Not every consumer of FBI CJIS services will encounter all of the policy areas therefore the circumstances of applicability are based on individual agency/entity configurations and usage. Use cases within each of the policy areas will help users relate the Policy to their own agency circumstances. The policy areas are:

- Information Exchange Agreements
- Access Control (AC)
- Awareness and Training (AT)
- Auditing and Accountability (AU)
- Assessment, Authorization, and Monitoring (CA)
- Configuration Management (CM)
- Contingency Planning (CP)
- Identification and Authentication (IA)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Physical and Environmental Protection (PE)
- Planning (PL)
- Personnel Security (PS)
- Risk Assessment (RA)
- System and Services Acquisition (SA)
- Systems and Communications Protection (SC)
- System and Information Integrity (SI)
- Supply Chain Risk Management (SR)
- Mobile Devices

5.1 Policy Area 1: Information Exchange Agreements

The information shared through communication mediums shall be protected with appropriate security safeguards. The agreements established by entities sharing information across systems and communications mediums are vital to ensuring all parties fully understand and agree to a set of security standards.

5.1.1 Information Exchange

Before exchanging CJI, agencies shall put formal agreements in place that specify security controls. The exchange of information may take several forms including electronic mail, instant messages, web services, facsimile, hard copy, and information systems sending, receiving and storing CJI.

Information exchange agreements outline the roles, responsibilities, and data ownership between agencies and any external parties. Information exchange agreements for agencies sharing CJI data that is sent to and/or received from the FBI CJIS shall specify the security controls and conditions described in this document.

Information exchange agreements shall be supported by documentation committing both parties to the terms of information exchange. As described in subsequent sections, different agreements and policies apply, depending on whether the parties involved are CJAs or NCJAs. See Appendix D for examples of Information Exchange Agreements.

5.1.2 Monitoring, Review, and Delivery of Services

As specified in the interagency agreements, MCAs, and contractual agreements with private contractors, the services, reports and records provided by the service provider shall be regularly monitored and reviewed. The CJA, authorized agency, or FBI shall maintain sufficient overall control and visibility into all security aspects to include, but not limited to, identification of vulnerabilities and information security incident reporting/response. The incident reporting/response process used by the service provider shall conform to the incident reporting/response specifications provided in this Policy.

5.1.2.1 Managing Changes to Service Providers

Any changes to services provided by a service provider shall be managed by the CJA, authorized agency, or FBI. This includes provision of services, changes to existing services, and new services. Evaluation of the risks to the agency shall be undertaken based on the criticality of the data, system, and the impact of the change.

Figure 3 – Information Exchange Agreements Implemented by a Local Police Department

A local police department executed a Memorandum of Understanding (MOU) for the interface with their state CSA. The local police department also executed an MOU (which included an MCA) with the county information technology (IT) department for the day-to-day operations of their criminal-justice infrastructure. The county IT department, in turn, outsourced operations to a local vendor who signed the CJIS Security Addendum.

ACCESS CONTROL (AC)

Access control provides the planning and implementation of mechanisms to restrict reading, writing, processing, and transmission of CJIS information and the modification of information systems, applications, services and communication configurations allowing access to CJIS information.

Refer to Section 5.13.6 for additional access control requirements related to mobile devices used to access CJI.

AC-1 POLICY AND PROCEDURES

[Priority 2]

Control:

- a. Develop, document, and disseminate to: organizational personnel with access control responsibilities
 1. Agency-level access control policy that:
 - (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 - (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
 2. Procedures to facilitate the implementation of the access control policy and the associated access controls;
- b. Designate an individual with security responsibilities to manage the development, documentation, and dissemination of the access control policy and procedures; and
- c. Review and update the current access control:
 1. Policy annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI; and
 2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.

Discussion: Access control policy and procedures address the controls in the AC family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of access control policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies reflecting the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to access control policy and procedures

include assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: IA-1, PS-8, SI-12.

AC-2 ACCOUNT MANAGEMENT

[Existing] [Priority 1]

Control:

- a. Define and document the types of accounts allowed and specifically prohibited for use within the system;
- b. Assign account managers;
- c. Require conditions for group and role membership;
- d. Specify:
 1. Authorized users of the system;
 2. Group and role membership; and
 3. Access authorizations (i.e., privileges) and attributes listed for each account;

Attribute Name

Email Address Text

Employer Name

Federation Id

Given Name

Identity Provider Id

Sur Name

Telephone Number

Identity Provider Id

Unique Subject Id

Counter Terrorism Data Self Search Home Privilege Indicator

Criminal History Data Self Search Home Privilege Indicator

Criminal Intelligence Data Self Search Home Privilege Indicator

Criminal Investigative Data Self Search Home Privilege Indicator

Display Name

Government Data Self Search Home Privilege Indicator

Local Id

NCIC Certification Indicator

N-DEx Privilege Indicator

PCII Certification Indicator

28 CFR Certification Indicator

Employer ORI

Employer Organization General Category Code

Employer State Code

Public Safety Officer Indicator

Sworn Law Enforcement Officer Indicator

Authenticator Assurance Level

Federation Assurance Level

Identity Assurance Level

Intelligence Analyst Indicator

- e. Require approvals by organizational personnel with account management responsibilities for requests to create accounts;
- f. Create, enable, modify, disable, and remove accounts in accordance with agency policy;
- g. Monitor the use of accounts;
- h. Notify account managers and system/network administrators within:
 - 1. One day when accounts are no longer required;
 - 2. One day when users are terminated or transferred; and
 - 3. One day when system usage or need-to-know changes for an individual;
- i. Authorize access to the system based on:
 - 1. A valid access authorization;

2. Intended system usage; and
 3. Attributes as listed in AC-2(d)(3);
- j. Review accounts for compliance with account management requirements at least annually;
 - k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and
 - l. Align account management processes with personnel termination and transfer processes.

Discussion: Examples of system account types include individual, shared, group, system, guest, anonymous, emergency, developer, temporary, and service. Identification of authorized system users and the specification of access privileges reflect the requirements in other controls in the security plan. Users requiring administrative privileges on system accounts receive additional scrutiny by organizational personnel responsible for approving such accounts and privileged access, including system owner, mission or business owner, senior agency information security officer, or senior agency official for privacy. Types of accounts that organizations may wish to prohibit due to increased risk include shared, group, emergency, anonymous, temporary, and guest accounts. Where access involves personally identifiable information, security programs collaborate with the senior agency official for privacy to establish the specific conditions for group and role membership; specify authorized users, group and role membership, and access authorizations for each account; and create, adjust, or remove system accounts in accordance with organizational policies. Policies can include such information as account expiration dates or other factors that trigger the disabling of accounts. Organizations may choose to define access privileges or other attributes by account, type of account, or a combination of the two. Examples of other attributes required for authorizing access include restrictions on time of day, day of week, and point of origin. In defining other system account attributes, organizations consider system-related requirements and mission/business requirements. Failure to consider these factors could affect system availability.

Temporary and emergency accounts are intended for short-term use. Organizations establish temporary accounts as part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation. Organizations establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency and temporary accounts are not to be confused with infrequently used accounts, including local logon accounts used for special tasks or when network resources are unavailable (may also be known as accounts of last resort). Such accounts remain available and are not subject to automatic disabling or removal dates. Conditions for disabling or deactivating accounts include when shared/group, emergency, or temporary accounts are no longer required and when individuals are transferred or terminated. Changing shared/group authenticators when members leave the group is intended to ensure that former group members do not retain access to the shared or group account. Some types of system accounts may require specialized training.

Related Controls: AC-3, AC-5, AC-6, AC-17, AC-18, AC-20, AU-2, AU-12, CM-5, IA-2, IA-4, IA-5, IA-8, MA-3, MA-5, PE-2, PL-4, PS-2, PS-4, PS-5, SC-7, SC-12, SC-13.

Control Enhancements:

(1) ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT

[Priority 1]

Control:

Support the management of system accounts using automated mechanisms including email, phone, and text notifications.

Discussion: Automated system account management includes using automated mechanisms to create, enable, modify, disable, and remove accounts; notify account managers when an account is created, enabled, modified, disabled, or removed, or when users are terminated or transferred; monitor system account usage; and report atypical system account usage.

Automated mechanisms can include internal system functions and email, telephonic, and text messaging notifications.

Related Controls: None.

(2) ACCOUNT MANAGEMENT | AUTOMATED TEMPORARY AND EMERGENCY ACCOUNT MANAGEMENT

[Priority 1]

Control:

Automatically remove temporary and emergency accounts within 72 hours.

Discussion: Management of temporary and emergency accounts includes the removal or disabling of such accounts automatically after a predefined time period rather than at the convenience of the system administrator. Automatic removal or disabling of accounts provides a more consistent implementation.

Related Controls: None.

(3) ACCOUNT MANAGEMENT | DISABLE ACCOUNTS

[Priority 1]

Control:

Disable accounts within one (1) week when the accounts:

- a. Have expired;
- b. Are no longer associated with a user or individual;
- c. Are in violation of organizational policy; or
- d. Have been inactive for 90 calendar days.

Discussion: Disabling expired, inactive, or otherwise anomalous accounts supports the concepts of least privilege and least functionality which reduce the attack surface of the system.

Related Controls: None.

(4) ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS

[Existing] [Priority 1]

Control:

Automatically audit account creation, modification, enabling, disabling, and removal actions.

Discussion: Account management audit records are defined in accordance with AU-2 and reviewed, analyzed, and reported in accordance with AU-6.

Related Controls: AU-2, AU-6.

(5) ACCOUNT MANAGEMENT | INACTIVITY LOGOUT

[Priority 1]

Control:

Require that users log out when a work period has been completed.

Discussion: Inactivity logout is behavior- or policy-based and requires users to take physical action to log out when they are expecting inactivity longer than the defined period. Automatic enforcement of inactivity logout is addressed by AC-11.

Related Controls: AC-11.

(13) ACCOUNT MANAGEMENT | DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS

[Priority 1]

Control:

Disable accounts of individuals within 30 minutes of discovery of direct threats to the confidentiality, integrity, or availability of CJI.

Discussion: Users who pose a significant security and/or privacy risk include individuals for whom reliable evidence indicates either the intention to use authorized access to systems to cause harm or through whom adversaries will cause harm. Such harm includes adverse impacts to organizational operations, organizational assets, individuals, other organizations, or the Nation. Close coordination among system administrators, legal staff, human resource managers, and authorizing officials is essential when disabling system accounts for high-risk individuals.

Related Controls: AU-6, SI-4.

AC-3 ACCESS ENFORCEMENT

[Existing] [Priority 1]

Control:

Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

Discussion: Access control policies control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (i.e., devices, files, records, domains) in organizational systems. In addition to enforcing authorized access at the system level and recognizing that systems can host many applications and services in support of mission and business functions, access enforcement mechanisms can also be employed at the application and service level to provide increased information security and privacy. In contrast to logical access controls that are implemented within the system, physical access controls are addressed by the controls in the Physical and Environmental Protection (PE) family.

Related Controls: AC-2, AC-4, AC-5, AC-6, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AT-2, AT-3, AU-9, CA-9, CM-5, CM-11, IA-2, IA-5, IA-6, IA-7, IA-11, MA-3, MA-4, MA-5, MP-4, PS-3, SC-2, SC-4, SC-12, SC-13, SC-28, SI-4, SI-8.

Control Enhancements:

(14) ACCESS ENFORCEMENT | INDIVIDUAL ACCESS

[Existing] [Priority 1]

Control:

Provide automated or manual processes to enable individuals to have access to elements of their personally identifiable information.

Discussion: Individual access affords individuals the ability to review personally identifiable information about them held within organizational records, regardless of format. Access helps individuals to develop an understanding about how their personally identifiable information is being processed. It can also help individuals ensure that their data is accurate. Access mechanisms can include request forms and application interfaces. For federal agencies, [PRIVACT] processes can be located in systems of record notices and on agency websites. Access to certain types of records may not be appropriate (e.g., for federal agencies, law enforcement records within a system of records may be exempt from disclosure under the [PRIVACT]) or may require certain levels of authentication assurance.

Organizational personnel consult with the senior agency official for privacy and legal counsel to determine appropriate mechanisms and access rights or limitations.

Related Controls: IA-8.

AC-4 INFORMATION FLOW ENFORCEMENT

[Existing] [Priority 1]

Control:

Enforce approved authorizations for controlling the flow of information within the system and between connected systems by preventing CJI from being transmitted unencrypted across the public network, blocking outside traffic that claims to be from within the agency, and not passing any web requests to the public network that are not from the agency-controlled or internal boundary protection devices (e.g., proxies, gateways, firewalls, or routers).

Discussion: Information flow control regulates where information can travel within a system and between systems (in contrast to who is allowed to access the information) and without regard to subsequent accesses to that information. Flow control restrictions include blocking external traffic that claims to be from within the organization, keeping export-controlled information from being transmitted in the clear to the Internet, restricting web requests that are not from the internal web proxy server, and limiting information transfers between organizations based on data structures and content. Transferring information between organizations may require an agreement specifying how the information flow is enforced (see CA-3). Transferring information between systems in different security or privacy domains with different security or privacy policies introduces the risk

that such transfers violate one or more domain security or privacy policies. In such situations, information owners/stewards provide guidance at designated policy enforcement points between connected systems. Organizations consider mandating specific architectural solutions to enforce specific security and privacy policies. Enforcement includes prohibiting information transfers between connected systems (i.e., allowing access only), verifying write permissions before accepting information from another security or privacy domain or connected system, employing hardware mechanisms to enforce one-way information flows, and implementing trustworthy regrading mechanisms to reassign security or privacy attributes and labels.

Organizations commonly employ information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations within systems and between connected systems. Flow control is based on the characteristics of the information and/or the information path. Enforcement occurs, for example, in boundary protection devices that employ rule sets or establish configuration settings that restrict system services, provide a packet-filtering capability based on header information, or provide a message-filtering capability based on message content. Organizations also consider the trustworthiness of filtering and/or inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement. Control enhancements 3 through 32 primarily address cross-domain solution needs that focus on more advanced filtering techniques, in-depth analysis, and stronger flow enforcement mechanisms implemented in cross-domain products, such as high-assurance guards. Such capabilities are generally not available in commercial off-the-shelf products. Information flow enforcement also applies to control plane traffic (e.g., routing and DNS).

Related Controls: AC-3, AC-6, AC-17, AC-19, AC-21, CA-3, CA-9, CM-7, SC-4, SC-7.

AC-5 SEPARATION OF DUTIES

[Existing] [Priority 1]

Control:

- a. Identify and document separation of duties based on specific duties, operations, or information systems, as necessary, to mitigate risk to CJI; and
- b. Define system access authorizations to support separation of duties.

Discussion: Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes dividing mission or business functions and support functions among different individuals or roles, conducting system support functions with different individuals, and ensuring that security personnel who administer access control functions do not also administer audit functions.

Because separation of duty violations can span systems and application domains, organizations consider the entirety of systems and system components when developing policy on separation of duties. Separation of duties is enforced through the account management activities in AC-2, access control mechanisms in AC-3, and identity management activities in IA-2, IA-4, and IA-12.

Related Controls: AC-2, AC-3, AC-6, AU-9, CM-5, CM-11, CP-9, IA-2, IA-4, IA-5, IA-12, MA-3, MA-5, PS-2, SA-8.

AC-6 LEAST PRIVILEGE

[Existing] [Priority 1]

Control:

Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.

Discussion: Organizations employ least privilege for specific duties and systems. The principle of least privilege is also applied to system processes, ensuring that the processes have access to systems and operate at privilege levels no higher than necessary to accomplish organizational missions or business functions. Organizations consider the creation of additional processes, roles, and accounts as necessary to achieve least privilege. Organizations apply least privilege to the development, implementation, and operation of organizational systems.

Related Controls: AC-2, AC-3, AC-5, CM-5, CM-11, PL-2, SA-8, SA-15.

Control Enhancements:

(1) LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS

[Existing] [Priority 1]

Control:

Authorize access for personnel including security administrators, system and network administrators, and other privileged users with access to system control, monitoring, or administration functions (e.g., system administrators, information security personnel, maintainers, system programmers, etc.) to:

- a. Established system accounts, configured access authorizations (i.e., permissions, privileges), set events to be audited, set intrusion detection parameters, and other security functions; and
- b. Security-relevant information in hardware, software, and firmware.

Discussion: Security functions include establishing system accounts, configuring access authorizations (i.e., permissions, privileges), configuring settings for events to be audited, and establishing intrusion detection parameters. Security-relevant information includes filtering rules for routers or firewalls, configuration parameters for security services, cryptographic key management information, and access control lists. Authorized personnel include security administrators, system administrators, system security officers, system programmers, and other privileged users.

Related Controls: AC-17, AC-18, AC-19, AU-9, PE-2.

(2) LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS

[Existing] [Priority 1]

Control:

Require that users of system accounts (or roles) with access to privileged security functions or security-relevant information (e.g., audit logs), use non-privileged accounts or roles, when accessing non-security functions.

Discussion: Requiring the use of non-privileged accounts when accessing non-security functions limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies, such as role-based access control, and where a change of role provides the same degree of assurance in the change of access authorizations for the user and the processes acting on behalf of the user as would be provided by a change between a privileged and non- privileged account.

Related Controls: AC-17, AC-18, AC-19, PL-4.

(5) LEAST PRIVILEGE | PRIVILEGED ACCOUNTS

[Existing] [Priority 1]

Control:

Restrict privileged accounts on the system to privileged users.

Discussion: Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from accessing privileged information or privileged functions. Organizations may differentiate in the application of restricting privileged accounts between allowed privileges for local accounts and for domain accounts provided that they retain the ability to control system configurations for key parameters and as otherwise necessary to sufficiently mitigate risk.

Related Controls: IA-2, MA-3, MA-4.

(7) LEAST PRIVILEGE | REVIEW OF USER PRIVILEGES

[Existing] [Priority 1]

Control:

- a. Review annually the privileges assigned to non-privileged and privileged users to validate the need for such privileges; and
- b. Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs.

Discussion: The need for certain assigned user privileges may change over time to reflect changes in organizational mission and business functions, environments of operation, technologies, or threats. A periodic review of assigned user privileges is necessary to determine if the rationale for assigning such privileges remains valid. If the need cannot be revalidated, organizations take appropriate corrective actions.

Related Controls: CA-7.

(9) LEAST PRIVILEGE | LOG USE OF PRIVILEGED FUNCTIONS

[Existing] [Priority 1]

Control:

Log the execution of privileged functions.

Discussion: The misuse of privileged functions, either intentionally or unintentionally by authorized users or by unauthorized external entities that have compromised system accounts, is a

serious and ongoing concern and can have significant adverse impacts on organizations. Logging and analyzing the use of privileged functions is one way to detect such misuse and, in doing so, help mitigate the risk from insider threats and the advanced persistent threat.

Related Controls: AU-2, AU-3, AU-12.

(10) LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS

[Existing] [Priority 1]

Control:

Prevent non-privileged users from executing privileged functions.

Discussion: Privileged functions include disabling, circumventing, or altering implemented security or privacy controls, establishing system accounts, performing system integrity checks, and administering cryptographic key management activities. Non-privileged users are individuals who do not possess appropriate authorizations. Privileged functions that require protection from non-privileged users include circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms. Preventing non-privileged users from executing privileged functions is enforced by AC-3.

Related Controls: None.

AC-7 UNSUCCESSFUL LOGON ATTEMPTS

[Existing] [Priority 3]

Control:

- a. Enforce a limit of five (5) consecutive invalid logon attempts by a user during a 15-minute time period; and
- b. Automatically lock the account or node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.

Discussion: The need to limit unsuccessful logon attempts and take subsequent action when the maximum number of attempts is exceeded applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by systems are usually temporary and automatically release after a predetermined, organization-defined time period. If a delay algorithm is selected, organizations may employ different algorithms for different components of the system based on the capabilities of those components. Responses to unsuccessful logon attempts may be implemented at the operating system and the application levels. Organization-defined actions that may be taken when the number of allowed consecutive invalid logon attempts is exceeded include prompting the user to answer a secret question in addition to the username and password, invoking a lockdown mode with limited user capabilities (instead of full lockout), allowing users to only logon from specified Internet Protocol (IP) addresses, requiring a CAPTCHA to prevent automated attacks, or applying user profiles such as location, time of day, IP address, device, or Media Access Control (MAC) address. If automatic system lockout or execution of a delay algorithm is not implemented in support of the availability objective, organizations consider a combination of other actions to help prevent brute force attacks.

In addition to the above, organizations can prompt users to respond to a secret question before the number of allowed unsuccessful logon attempts is exceeded. Automatically unlocking an account after a specified period of time is generally not permitted. However, exceptions may be required based on operational mission or need.

Related Controls: AC-2, AU-2, AU-6, IA-5.

AC-8 SYSTEM USE NOTIFICATION

[Existing] [Priority 2]

Control:

- a. Display a system use notification message to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that:
 1. Users are accessing a restricted information system;
 2. System usage may be monitored, recorded, and subject to audit;
 3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and
 4. Use of the system indicates consent to monitoring and recording;
- b. Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system; and
- c. For publicly accessible systems:
 1. Display system use information consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines, before granting further access to the publicly accessible system;
 2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
 3. Include a description of the authorized uses of the system.

Discussion: System use notifications can be implemented using messages or warning banners displayed before individuals log in to systems. System use notifications are used only for access via logon interfaces with human users. Notifications are not required when human interfaces do not exist. Based on an assessment of risk, organizations consider whether or not a secondary system use notification is needed to access applications or other system resources after the initial network logon. Organizations consider system use notification messages or banners displayed in multiple languages based on organizational needs and the demographics of system users. Organizations consult with the privacy office for input regarding privacy messaging and the Office of the General Counsel or organizational equivalent for legal review and approval of warning banner content.

Related Controls: AC-14, PL-4, SI-4.

AC-11 DEVICE LOCK

[Existing] [Priority 4]

Control:

- a. Prevent further access to the system by initiating a device lock after a maximum of 30 minutes of inactivity and requiring the user to initiate a device lock before leaving the system unattended.

NOTE: In the interest of safety, devices that are: (1) part of a criminal justice conveyance; or (2) used to perform dispatch functions and located within a physically secure location; or (3) terminals designated solely for the purpose of receiving alert notifications (i.e., receive only terminals or ROT) used within physically secure location facilities that remain staffed when in operation, are exempt from this requirement.

- b. Retain the device lock until the user reestablishes access using established identification and authentication procedures.

Discussion: Device locks are temporary actions taken to prevent logical access to organizational systems when users stop work and move away from the immediate vicinity of those systems but do not want to log out because of the temporary nature of their absences. Device locks can be implemented at the operating system level or at the application level. A proximity lock may be used to initiate the device lock (e.g., via a Bluetooth-enabled device or dongle). User-initiated device locking is behavior or policy-based and, as such, requires users to take physical action to initiate the device lock. Device locks are not an acceptable substitute for logging out of systems, such as when organizations require users to log out at the end of workdays.

Related Controls: AC-2, AC-7, IA-11, PL-4.

Control Enhancements:

(1) DEVICE LOCK | PATTERN-HIDING DISPLAYS

[Existing] [Priority 4]

Control:

Conceal, via the device lock, information previously visible on the display with a publicly viewable image.

Discussion: The pattern-hiding display can include static or dynamic images, such as patterns used with screen savers, photographic images, solid colors, clock, battery life indicator, or a blank screen with the caveat that controlled unclassified information is not displayed.

Related Controls: None.

AC-12 SESSION TERMINATION

[Priority 3]

Control:

Automatically terminate a user session after a user has been logged out.

Discussion: Session termination addresses the termination of user-initiated logical sessions (in contrast to SC-10, which addresses the termination of network connections associated with communications sessions [i.e., network disconnect]). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational system. Such user sessions can be terminated without terminating network sessions. Session termination ends all processes associated with a user's logical session except for those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated. Conditions or trigger events that require automatic termination of the session include organization-defined periods of user inactivity, targeted responses to certain types of incidents, or time-of-day restrictions on system use.

Related Controls: MA-4, SC-10, SC-23.

AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

[Priority 4]

Control:

- a. Identify any specific user actions that can be performed on the system without identification or authentication consistent with organizational mission and business functions; and
- b. Document and provide supporting rationale in the security plan for the system, user actions not requiring identification or authentication.

Discussion: Specific user actions may be permitted without identification or authentication if organizations determine that identification and authentication are not required for the specified user actions. Organizations may allow a limited number of user actions without identification or authentication, including when individuals access public websites or other publicly accessible federal systems, when individuals use mobile phones to receive calls, or when facsimiles are received. Organizations identify actions that normally require identification or authentication but may, under certain circumstances, allow identification or authentication mechanisms to be bypassed. Such bypasses may occur, for example, via a software-readable physical switch that commands bypass of the logon functionality and is protected from accidental or unmonitored use. Permitting actions without identification or authentication does not apply to situations where identification and authentication have already occurred and are not repeated but rather to situations where identification and authentication have not yet occurred. Organizations may decide that there are no user actions that can be performed on organizational systems without identification and authentication, and therefore, the value for the assignment operation can be "none."

Related Controls: AC-8, IA-2, PL-2.

AC-17 REMOTE ACCESS

[Existing] [Priority 1]

Control:

- a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and

- b. Authorize each type of remote access to the system prior to allowing such connections.

Discussion: Remote access is access to organizational systems (or processes acting on behalf of users) that communicate through external networks such as the Internet. Types of remote access include dial-up, broadband, and wireless. Organizations use encrypted virtual private networks (VPNs) to enhance confidentiality and integrity for remote connections. The use of encrypted VPNs provides sufficient assurance to the organization that it can effectively treat such connections as internal networks if the cryptographic mechanisms used are implemented in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Still, VPN connections traverse external networks, and the encrypted VPN does not enhance the availability of remote connections. VPNs with encrypted tunnels can also affect the ability to adequately monitor network communications traffic for malicious code. Remote access controls apply to systems other than public web servers or systems designed for public access. Authorization of each remote access type addresses authorization prior to allowing remote access without specifying the specific formats for such authorization. While organizations may use information exchange and system connection security agreements to manage remote access connections to other systems, such agreements are addressed as part of CA-3. Enforcing access restrictions for remote access is addressed via AC-3.

Related Controls: AC-2, AC-3, AC-4, AC-18, AC-19, AC-20, CA-3, CM-10, IA-2, IA-3, IA-8, MA-4, PE- 17, PL-2, PL-4, SC-10, SC-12, SC-13, SI-4.

Control Enhancements:

(1) REMOTE ACCESS | MONITORING AND CONTROL

[Existing] [Priority 1]

Control:

Employ automated mechanisms to monitor and control remote access methods.

Discussion: Monitoring and control of remote access methods allows organizations to detect attacks and help ensure compliance with remote access policies by auditing the connection activities of remote users on a variety of system components, including servers, notebook computers, workstations, smart phones, and tablets. Audit logging for remote access is enforced by AU-2. Audit events are defined in AU-2a.

Related Controls: AU-2, AU-6, AU-12.

(2) REMOTE ACCESS | PROTECTION OF CONFIDENTIALITY AND INTEGRITY USING ENCRYPTION

[Existing] [Priority 1]

Control:

Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

Discussion: Virtual private networks can be used to protect the confidentiality and integrity of remote access sessions. Transport Layer Security (TLS) is an example of a cryptographic protocol

that provides end-to-end communications security over networks and is used for Internet communications and online transactions.

Related Controls: SC-8, SC-12, SC-13.

(3) REMOTE ACCESS | MANAGED ACCESS CONTROL POINTS

[Existing] [Priority 1]

Control:

Route remote accesses through authorized and managed network access control points.

Discussion: Organizations consider the Trusted Internet Connections (TIC) initiative requirements for external network connections since limiting the number of access control points for remote access reduces attack surfaces.

Related Controls: SC-7.

(4) REMOTE ACCESS | PRIVILEGED COMMANDS AND ACCESS

[Existing] [Priority 1]

Control:

- a. Authorize the execution of privileged commands and access to security-relevant information via remote access only in a format that provides assessable evidence and for the following needs: compelling operational needs; and
- b. Document the rationale for remote access in the security plan for the system.

Discussion: Remote access to systems represents a significant potential vulnerability that can be exploited by adversaries. As such, restricting the execution of privileged commands and access to security-relevant information via remote access reduces the exposure of the organization and the susceptibility to threats by adversaries to the remote access capability.

Related Controls: AC-6, SC-12, SC-13.

AC-18 WIRELESS ACCESS

[Existing] [Priority 2]

Control:

- a. Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access; and
- b. Authorize each type of wireless access to the system prior to allowing such connections.

Discussion: Wireless technologies include microwave, packet radio (ultra-high frequency or very high frequency), 802.11x, and Bluetooth. Wireless networks use authentication protocols that provide authenticator protection and mutual authentication.

Related Controls: AC-2, AC-3, AC-17, AC-19, CA-9, CM-7, IA-2, IA-3, IA-8, PL-4, SI-4.

Control Enhancements:

(1) WIRELESS ACCESS | AUTHENTICATION AND ENCRYPTION

[Existing] [Priority 2]

Control:

Protect wireless access to the system using authentication of authorized users and agency-controlled devices, and encryption.

Discussion: Wireless networking capabilities represent a significant potential vulnerability that can be exploited by adversaries. To protect systems with wireless access points, strong authentication of users and devices along with strong encryption can reduce susceptibility to threats by adversaries involving wireless technologies.

Related Controls: SC-8, SC-12, SC-13.

(3) WIRELESS ACCESS | DISABLE WIRELESS NETWORKING

[Existing] [Priority 2]

Control:

Disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment.

Discussion: Wireless networking capabilities that are embedded within system components represent a significant potential vulnerability that can be exploited by adversaries. Disabling wireless capabilities when not needed for essential organizational missions or functions can reduce susceptibility to threats by adversaries involving wireless technologies.

Related Controls: None.

AC-19 ACCESS CONTROL FOR MOBILE DEVICES

[Existing] [Priority 2]

Control:

- a. Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas; and
- b. Authorize the connection of mobile devices to organizational systems.

Discussion: A mobile device is a computing device that has a small form factor such that it can easily be carried by a single individual; is designed to operate without a physical connection; possesses local, non-removable or removable data storage; and includes a self-contained power source. Mobile device functionality may also include voice communication capabilities, on-board sensors that allow the device to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones and tablets. Mobile devices are typically associated with a single individual. The processing, storage, and transmission capability of the mobile device may be comparable to or merely a subset of notebook/desktop systems, depending on the nature and intended purpose of the device. Protection and control of mobile devices is behavior or policy-based and requires users to take physical action to protect and control such devices when outside of controlled areas. Controlled areas are spaces for which organizations

provide physical or procedural controls to meet the requirements established for protecting information and systems. Due to the large variety of mobile devices with different characteristics and capabilities, organizational restrictions may vary for the different classes or types of such devices. Usage restrictions and specific implementation guidance for mobile devices include configuration management, device identification and authentication, implementation of mandatory protective software, scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware.

Usage restrictions and authorization to connect may vary among organizational systems. For example, the organization may authorize the connection of mobile devices to its network and impose a set of usage restrictions, while a system owner may withhold authorization for mobile device connection to specific applications or impose additional usage restrictions before allowing mobile device connections to a system. Adequate security for mobile devices goes beyond the requirements specified in AC-19. Many safeguards for mobile devices are reflected in other controls. AC-20 addresses mobile devices that are not organization-controlled.

Related Controls: AC-3, AC-4, AC-7, AC-11, AC-17, AC-18, AC-20, CA-9, CM-2, CM-6, IA-2, IA-3, MP-2, MP-4, MP-5, MP-7, PL-4, SC-7, SI-3, SI-4.

Control Enhancements:

(5) ACCESS CONTROL FOR MOBILE DEVICES | FULL DEVICE OR CONTAINER-BASED ENCRYPTION

[Existing] [Priority 2]

Control:

Employ full-device encryption to protect the confidentiality and integrity of information on full- and limited-feature operating system mobile devices authorized to process, store, or transmit CJI.

Discussion: Container-based encryption provides a more fine-grained approach to data and information encryption on mobile devices, including encrypting selected data structures such as files, records, or fields.

Related Controls: SC-12, SC-13, SC-28.

AC-20 USE OF EXTERNAL SYSTEMS

[Existing] [Priority 1]

Control:

- a. Establish agency-level policies governing the use of external systems consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to:
 1. Access the system from external systems; and
 2. Process, store, or transmit organization-controlled information using external systems; or
- b. Prohibit the use of personally-owned information systems including mobile devices (i.e.,

bring your own device [BYOD]) and publicly accessible systems for accessing, processing, storing, or transmitting CJI.

Discussion: External systems are systems that are used by but not part of organizational systems, and for which the organization has no direct control over the implementation of required controls or the assessment of control effectiveness. External systems include personally-owned systems, components, or devices; privately owned computing and communications devices in commercial or public facilities; systems owned or controlled by nonfederal organizations; systems managed by contractors; and federal information systems that are not owned by, operated by, or under the direct supervision or authority of the organization. External systems also include systems owned or operated by other components within the same organization and systems within the organization with different authorization boundaries. Organizations have the option to prohibit the use of any type of external system or prohibit the use of specified types of external systems, (e.g., prohibit the use of any external system that is not organizationally owned or prohibit the use of personally-owned systems).

For some external systems (i.e., systems operated by other organizations), the trust relationships that have been established between those organizations and the originating organization may be such that no explicit terms and conditions are required. Systems within these organizations may not be considered external. These situations occur when, for example, there are pre-existing information exchange agreements (either implicit or explicit) established between organizations or components or when such agreements are specified by applicable laws, executive orders, directives, regulations, policies, or standards. Authorized individuals include organizational personnel, contractors, or other individuals with authorized access to organizational systems and over which organizations have the authority to impose specific rules of behavior regarding system access. Restrictions that organizations impose on authorized individuals need not be uniform, as the restrictions may vary depending on trust relationships between organizations.

Therefore, organizations may choose to impose different security restrictions on contractors than on state, local, or tribal governments.

External systems used to access public interfaces to organizational systems are outside the scope of AC-20. Organizations establish specific terms and conditions for the use of external systems in accordance with organizational security policies and procedures. At a minimum, terms and conditions address the specific types of applications that can be accessed on organizational systems from external systems and the highest security category of information that can be processed, stored, or transmitted on external systems. If the terms and conditions with the owners of the external systems cannot be established, organizations may impose restrictions on organizational personnel using those external systems.

Related Controls: AC-2, AC-3, AC-17, AC-19, CA-3, PL-2, PL-4, SA-9, SC-7.

Control Enhancements:

(1) USE OF EXTERNAL SYSTEMS | LIMITS ON AUTHORIZED USE

[Priority 1]

Control:

Permit authorized individuals to use an external system to access the system or to process, store, or transmit organization-controlled information only after:

- a. Verification of the implementation of controls on the external system as specified in the organization's security and privacy policies and security and privacy plans; or
- b. Retention of approved system connection or processing agreements with the organizational entity hosting the external system.

Discussion: Limiting authorized use recognizes circumstances where individuals using external systems may need to access organizational systems. Organizations need assurance that the external systems contain the necessary controls so as not to compromise, damage, or otherwise harm organizational systems. Verification that the required controls have been implemented can be achieved by external, independent assessments, attestations, or other means, depending on the confidence level required by organizations.

Related Controls: CA-2.

(2) USE OF EXTERNAL SYSTEMS | PORTABLE STORAGE DEVICES — RESTRICTED USE

[Priority 1]

Control:

Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems.

Discussion: Limits on the use of organization-controlled portable storage devices in external systems include restrictions on how the devices may be used and under what conditions the devices may be used.

Related Controls: MP-7.

AC-21 INFORMATION SHARING

[Existing] [Priority 3]

Control:

- a. Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions as defined in an executed information exchange agreement; and
- b. Employ attribute-based access control (see AC-2(d)(3)) or manual processes as defined in information exchange agreements to assist users in making information sharing and collaboration decisions.

Discussion: Information sharing applies to information that may be restricted in some manner based on some formal or administrative determination. Examples of such information include, contract-sensitive information, classified information related to special access programs or compartments, privileged information, proprietary information, and personally identifiable information. Security and privacy risk assessments as well as applicable laws, regulations, and policies can provide useful inputs to these determinations. Depending on the circumstances, sharing partners may be defined at the individual, group, or organizational level. Information may

be defined by content, type, security category, or special access program or compartment. Access restrictions may include non-disclosure agreements (NDA). Information flow techniques and security attributes may be used to provide automated assistance to users making sharing and collaboration decisions.

Related Controls: AC-3, AC-4, RA-3, SC-15.

AC-22 PUBLICLY ACCESSIBLE CONTENT

[Priority 4]

Control:

- a. Designate individuals authorized to make information publicly accessible;
- b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information;
- c. Review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included; and
- d. Review the content on the publicly accessible system for nonpublic information quarterly and remove such information, if discovered.

Discussion: In accordance with applicable laws, executive orders, directives, policies, regulations, standards, and guidelines, the public is not authorized to have access to nonpublic information, including information protected under the [PRIVACT] and proprietary information. Publicly accessible content addresses systems that are controlled by the organization and accessible to the public, typically without identification or authentication. Posting information on non-organizational systems (e.g., non-organizational public websites, forums, and social media) is covered by organizational policy. While organizations may have individuals who are responsible for developing and implementing policies about the information that can be made publicly accessible, publicly accessible content addresses the management of the individuals who make such information publicly accessible.

Related Controls: AC-3, AT-2, AT3.

AWARENESS AND TRAINING (AT)

Security training is key to the human element of information security. All users with authorized access to CJI should be made aware of their individual responsibilities and expected behavior when accessing CJI and the systems which process CJI. LASOs require enhanced training on the specific duties and responsibilities of those positions and the impact those positions have on the overall security of information systems.

AT-1 POLICY AND PROCEDURES

[Priority 2]

Control:

- a. Develop, document, and disseminate to all personnel when their unescorted logical or physical access to any information system results in the ability, right, or privilege to view, modify, or make use of unencrypted CJI:
 1. Organization-level awareness and training policy that:
 - a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 - b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
 2. Procedures to facilitate the implementation of the awareness and training policy and the associated awareness and training controls;
- b. Designate organizational personnel with information security awareness and training responsibilities to manage the development, documentation, and dissemination of the awareness and training policy and procedures; and
- c. Review and update the current awareness and training:
 1. Policy annually and following changes in the information system operating environment, when security incidents occur, or when changes to the CJIS Security Policy are made; and
 2. Procedures annually and following changes in the information system operating environment, when security incidents occur, or when changes to the CJIS Security Policy are made.

Discussion: Awareness and training policy and procedures address the controls in the AT family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of awareness and training policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or

role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to awareness and training policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PS-8, SI-12.

AT-2 LITERACY TRAINING AND AWARENESS

[Existing] [Priority 2]

Control:

- a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors):
 1. As part of initial training for new users prior to accessing CJI and annually thereafter; and
 2. When required by system changes or within 30 days of any security event for individuals involved in the event;
- b. Employ one or more of the following techniques to increase the security and privacy awareness of system users:
 1. Displaying posters
 2. Offering supplies inscribed with security and privacy reminders
 3. Displaying logon screen messages
 4. Generating email advisories or notices from organizational officials
 5. Conducting awareness events
- c. Update literacy training and awareness content annually and following changes in the information system operating environment, when security incidents occur, or when changes are made in the CJIS Security Policy; and
- d. Incorporate lessons learned from internal or external security incidents or breaches into literacy training and awareness techniques.

Discussion: Organizations provide basic and advanced levels of literacy training to system users, including measures to test the knowledge level of users. Organizations determine the content of literacy training and awareness based on specific organizational requirements, the systems to which personnel have authorized access, and work environments (e.g., telework). The content includes an understanding of the need for security and privacy as well as actions by users to maintain security and personal privacy and to respond to suspected incidents. The content addresses the need for operations security and the handling of personally identifiable information.

Awareness techniques include displaying posters, offering supplies inscribed with security and privacy reminders, displaying logon screen messages, generating email advisories or notices

from organizational officials, and conducting awareness events. Literacy training after the initial training described in AT-2a.1 is conducted at a minimum frequency consistent with applicable laws, directives, regulations, and policies. Subsequent literacy training may be satisfied by one or more short ad hoc sessions and include topical information on recent attack schemes, changes to organizational security and privacy policies, revised security and privacy expectations, or a subset of topics from the initial training. Updating literacy training and awareness content on a regular basis helps to ensure that the content remains relevant. Events that may precipitate an update to literacy training and awareness content include, but are not limited to, assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Related Controls: AC-3, AC-17, AC-22, AT-3, AT-4, CP-3, IA-4, IR-2, IR-7, PL-4, PS-7, SA-8.

Control Enhancements:

(2) LITERACY TRAINING AND AWARENESS | INSIDER THREAT

[Existing] [Priority 2]

Control:

Provide literacy training on recognizing and reporting potential indicators of insider threat.

Discussion: Potential indicators and possible precursors of insider threat can include behaviors such as inordinate, long-term job dissatisfaction; attempts to gain access to information not required for job performance; unexplained access to financial resources; bullying or harassment of fellow employees; workplace violence; and other serious violations of policies, procedures, directives, regulations, rules, or practices. Literacy training includes how to communicate the concerns of employees and management regarding potential indicators of insider threat through channels established by the organization and in accordance with established policies and procedures. Organizations may consider tailoring insider threat awareness topics to the role. For example, training for managers may be focused on changes in the behavior of team members, while training for employees may be focused on more general observations.

(3) LITERACY TRAINING AND AWARENESS | SOCIAL ENGINEERING AND MINING

[Existing] [Priority 2]

Control:

Provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining.

Discussion: Social engineering is an attempt to trick an individual into revealing information or taking an action that can be used to breach, compromise, or otherwise adversely impact a system. Social engineering includes phishing, pretexting, impersonation, baiting, quid pro quo, thread-jacking, social media exploitation, and tailgating. Social mining is an attempt to gather information about the organization that may be used to support future attacks.

Literacy training includes information on how to communicate the concerns of employees and management regarding potential and actual instances of social engineering and data mining through organizational channels based on established policies and procedures.

AT-3 ROLE-BASED TRAINING

[Existing] [Priority 2]

Control:

- a. Provide role-based security and privacy training to personnel with the following roles and responsibilities:
 - All individuals with unescorted access to a physically secure location;
 - General User: A user, but not a process, who is authorized to use an information system;
 - Privileged User: A user that is authorized (and, therefore, trusted) to perform security-relevant functions that general users are not authorized to perform;
 - Organizational Personnel with Security Responsibilities: Personnel with the responsibility to ensure the confidentiality, integrity, and availability of CJI and the implementation of technology in a manner compliant with the CJISSECPOL.
 1. Before authorizing access to the system, information, or performing assigned duties, and annually thereafter; and
 2. When required by system changes.
- b. Update role-based training content annually and following audits of the CSA and local agencies; changes in the information system operating environment; security incidents; or when changes are made to the CJIS Security Policy;
- c. Incorporate lessons learned from internal or external security incidents or breaches into role-based training;
- d. Incorporate the minimum following topics into the appropriate role-based training content:
 1. All individuals with unescorted access to a physically secure location
 - a. Access, Use and Dissemination of Criminal History Record Information (CHRI), NCIC Restricted Files Information, and NCIC Non-Restricted Files Information Penalties
 - b. Reporting Security Events
 - c. Incident Response Training
 - d. System Use Notification
 - e. Physical Access Authorizations
 - f. Physical Access Control
 - g. Monitoring Physical Access
 - h. Visitor Control
 - i. Personnel Sanctions
 2. General User: A user, but not a process, who is authorized to use an information system. In addition to AT-3 (d) (1) above, include the following topics:
 - a. Criminal Justice Information

- b. Proper Access, Use, and Dissemination of NCIC Non-Restricted Files Information
 - c. Personally Identifiable Information
 - d. Information Handling
 - e. Media Storage
 - f. Media Access
 - g. Audit Monitoring, Analysis, and Reporting
 - h. Access Enforcement
 - i. Least Privilege
 - j. System Access Control
 - k. Access Control Criteria
 - l. System Use Notification
 - m. Session Lock
 - n. Personally Owned Information Systems
 - o. Password
 - p. Access Control for Display Medium
 - q. Encryption
 - r. Malicious Code Protection
 - s. Spam and Spyware Protection
 - t. Cellular Devices
 - u. Mobile Device Management
 - v. Wireless Device Risk Mitigations
 - w. Wireless Device Malicious Code Protection
 - x. Literacy Training and Awareness/Social Engineering and Mining
 - y. Identification and Authentication (Organizational Users)
 - z. Media Protection
3. Privileged User: A user that is authorized (and, therefore, trusted) to perform security-relevant functions that general users are not authorized to perform. In addition to AT-3 (d) (1) and (2) above, include the following topics:
- a. Access Control
 - b. System and Communications Protection and Information Integrity
 - c. Patch Management
 - d. Data backup and storage—centralized or decentralized approach
 - e. Most recent changes to the CJIS Security Policy
4. Organizational Personnel with Security Responsibilities: Personnel with the responsibility to ensure the confidentiality, integrity, and availability of CJI and the implementation of technology in a manner compliant with the CJISSECPOL. In addition to AT-3 (d) (1), (2), and (3) above, include the following topics:
- a. Local Agency Security Officer Role
 - b. Authorized Recipient Security Officer Role
 - c. Additional state/local/tribal/territorial or federal agency roles and responsibilities
 - d. Summary of audit findings from previous state audits of local agencies
 - e. Findings from the last FBI CJIS Division audit

Discussion: Organizations determine the content of training based on the assigned roles and responsibilities of individuals as well as the security and privacy requirements of organizations

and the systems to which personnel have authorized access, including technical training specifically tailored for assigned duties. Roles that may require role-based training include senior leaders or management officials (e.g., head of agency/chief executive officer, chief information officer, senior accountable official for risk management, senior agency information security officer, senior agency official for privacy), system owners; authorizing officials; system security officers; privacy officers; acquisition and procurement officials; enterprise architects; systems engineers; software developers; systems security engineers; privacy engineers; system, network, and database administrators; auditors; personnel conducting configuration management activities; personnel performing verification and validation activities; personnel with access to system-level software; control assessors; personnel with contingency planning and incident response duties; personnel with privacy management responsibilities; and personnel with access to personally identifiable information.

Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical controls. Role-based training also includes policies, procedures, tools, methods, and artifacts for the security and privacy roles defined. Organizations provide the training necessary for individuals to fulfill their responsibilities related to operations and supply chain risk management within the context of organizational security and privacy programs. Role-based training also applies to contractors who provide services to federal agencies. Types of training include web-based and computer-based training, classroom-style training, and hands-on training (including micro-training). Updating role-based training on a regular basis helps to ensure that the content remains relevant and effective. Events that may precipitate an update to role-based training content include, but are not limited to, assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Related Controls: AC-3, AC-17, AC-22, AT-2, AT-4, CP-3, IR-2, IR-4, IR-7, PL-4, PS-7, PS-9, SA-3, SA-8, SA-11, SR-5, SR-6, SR-11.

Control Enhancements:

(5) ROLE-BASED TRAINING | PROCESSING PERSONALLY IDENTIFIABLE INFORMATION

[Priority 2]

Control:

Provide all personnel when their unescorted logical or physical access to any information system results in the ability, right, or privilege to view, modify, or make use of unencrypted CJI with initial and annual training in the employment and operation of personally identifiable information processing and transparency controls.

Discussion: Personally identifiable information processing and transparency controls include the organization's authority to process personally identifiable information and personally identifiable information processing purposes. Role-based training for federal agencies addresses the types of information that may constitute personally identifiable information and the risks, considerations, and obligations associated with its processing. Such training also considers the authority to process personally identifiable information documented in privacy policies and notices, system of records notices, computer matching agreements and notices, privacy impact assessments,

[PRIVACT] statements, contracts, information sharing agreements, memoranda of understanding, and/or other documentation.

AT-4 TRAINING RECORDS

[Existing] [Priority 4]

Control:

- a. Document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training; and
- b. Retain individual training records for a minimum of three years.

Discussion: Documentation for specialized training may be maintained by individual supervisors at the discretion of the organization. The National Archives and Records Administration provides guidance on records retention for federal agencies. Retention of records for three (3) years accounts for a triennial audit cycle.

Related Controls: AT-2, AT-3, CP-3, IR-2, SI-12.

Figure 4 – Security Awareness Training Use Cases

Use Case 1 - Awareness and Training Program Implementation by a Local Police Department

A local police department with a staff of 20 sworn criminal justice professionals and 15 support personnel worked with a vendor to develop role-specific -awareness training, and required all staff to complete this training upon assignment and every year thereafter. The vendor maintained the training records for the police department's entire staff, and provided reporting to the department to help it ensure compliance with the CJIS Security Policy.

Use Case 2 – All individuals with unescorted access to a physically secure location

A local police department hires custodial staff that will have physical access throughout the PD (a physically secure location) after normal business hours to clean the facility. These personnel have unescorted access to a physically secure location and therefore must be given the awareness training on all the topics identified in CJISSECPOL AT-3 d 1.

Use Case 3 – General User Awareness and Training

A school district maintains a locked file cabinet with hard copies of background check results of all teachers and employees which may include CJI (CHRI). Only authorized personnel who have the ability to open the cabinet are required to be given the baseline security awareness training on all the topics identified in CJISSECPOL AT-3 d 1 and 2.

Use Case 4 – General User Awareness and Training

A County Sheriff's Office has employed a number of dispatchers. Part of the function of these dispatchers is to run CJI queries at the request of the Sheriff and deputies. As part of their daily duties, the dispatchers have access to CJI both logically (running queries) and physically (printed copies of reports containing CJI). These dispatchers are entrusted with direct access to CJI and are

therefore required to be given the awareness training on all the topics identified in CJISSECPOL AT-3 d 1 and 2.

Use Case 5 – Privileged User Awareness and Training

The State Police has hired a number of system and network administrator personnel to help bolster security of the state network. Part of their daily duties may include creating accounts for new personnel, implementing security patches for existing systems, creating backups of existing systems, and implementing access controls throughout the network. These administrators have privileged access to CJI and CJI-processing systems and are therefore required to be given the awareness training on all the topics identified in CJISSECPOL AT-3 d 1, 2, and 3.

AUDIT AND ACCOUNTABILITY (AU)

AU-1 POLICY AND PROCEDURES

[Existing] [Priority 2]

Control:

- a. Develop, document, and disseminate to organizational personnel with audit and accountability responsibilities:
 1. Agency and system-level audit and accountability policy that:
 - (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 - (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
 2. Procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls;
- b. Designate organizational personnel with information security responsibilities to manage the development, documentation, and dissemination of the audit and accountability policy and procedures; and
- c. Review and update the current audit and accountability:
 1. Policy annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI; and
 2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.

Discussion: Audit and accountability policy and procedures address the controls in the AU family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of audit and accountability policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to audit and accountability policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PS-8, SI-12.

AU-2 EVENT LOGGING

[Priority 2]

Control:

- a. Identify the types of events that the system is capable of logging in support of the audit function: authentication, file use, user/group management, events sufficient to establish what occurred, the sources of events, outcomes of events, and operational transactions (e.g., NCIC, III);
- b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;
- c. Specify the following event types for logging within the system:

All successful and unsuccessful:

1. System log-on attempts
2. Attempts to use:
 - a. Access permission on a user account, file, directory, or other system resource;
 - b. Create permission on a user account, file, directory, or other system resource;
 - c. Write permission on a user account, file, directory, or other system resource;
 - d. Delete permission on a user account, file, directory, or other system resource;
 - e. Change permission on a user account, file, directory, or other system resource.
3. Attempts to change account passwords
4. Actions by privileged accounts (i.e., root, Oracle, DBA, admin, etc.)
5. Attempts for users to:
 - a. Access the audit log file;
 - b. Modify the audit log file;
 - c. Destroy the audit log file.
- d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and
- e. Review and update the event types selected for logging annually.

Discussion: An event is an observable occurrence in a system. The types of events that require logging are those events that are significant and relevant to the security of systems and the privacy of individuals. Event logging also supports specific monitoring and auditing needs. Event types include password changes, failed logons or failed accesses related to systems, security or privacy attribute changes, administrative privilege usage, PIV credential usage, data action changes, query parameters, or external credential usage. In determining the set of event types that require logging, organizations consider the monitoring and auditing appropriate for

each of the controls to be implemented. For completeness, event logging includes all protocols that are operational and supported by the system.

To balance monitoring and auditing requirements with other system needs, event logging requires identifying the subset of event types that are logged at a given point in time. For example, organizations may determine that systems need the capability to log every file access successful and unsuccessful, but not activate that capability except for specific circumstances due to the potential burden on system performance. The types of events that organizations desire to be logged may change. Reviewing and updating the set of logged events is necessary to help ensure that the events remain relevant and continue to support the needs of the organization.

Organizations consider how the types of logging events can reveal information about individuals that may give rise to privacy risk and how best to mitigate such risks. For example, there is the potential to reveal personally identifiable information in the audit trail, especially if the logging event is based on patterns or time of usage.

Event logging requirements, including the need to log specific event types, may be referenced in other controls and control enhancements. These include AC-2(4), AC-3(10), AC-6(9), AC-17(1), CM-3f, CM-5(1), IA-3(3.b), MA-4(1), MP-4(2), PE-3, PM-21, PT-7, RA-8, SC-7(9), SC-7(15), SI-3(8), SI-4(22), SI-7(8), and SI-10(1). Organizations include event types that are required by applicable laws, executive orders, directives, policies, regulations, standards, and guidelines. Audit records can be generated at various levels, including at the packet level as information traverses the network. Selecting the appropriate level of event logging is an important part of a monitoring and auditing capability and can identify the root causes of problems. When defining event types, organizations consider the logging necessary to cover related event types, such as the steps in distributed, transaction-based processes and the actions that occur in service-oriented architectures.

Related Controls: AC-2, AC-3, AC-6, AC-7, AC-8, AC-17, AU-3, AU-4, AU-5, AU-6, AU-7, AU-11, AU-12, CM-3, CM-5, CM-6, IA-3, MA-4, MP-4, PE-3, SA-8, SC-7, SC-18, SI-3, SI-4, SI-7, SI-10, SI-11.

AU-3 CONTENT OF AUDIT RECORDS

[Existing] [Priority 2]

Control:

Ensure that audit records contain information that establishes the following:

- a. What type of event occurred;
- b. When the event occurred;
- c. Where the event occurred;
- d. Source of the event;
- e. Outcome of the event; and
- f. Identity of any individuals, subjects, or objects/entities associated with the event.

Discussion: Audit record content that may be necessary to support the auditing function includes event descriptions (item a), time stamps (item b), source and destination addresses (item c), user or process identifiers (items d and f), success or fail indications (item e), and filenames involved (items a, c, e, and f). Event outcomes include indicators of event success or failure and event-specific results, such as the system security and privacy posture after the event occurred.

Organizations consider how audit records can reveal information about individuals that may give rise to privacy risks and how best to mitigate such risks. For example, there is the potential to reveal personally identifiable information in the audit trail, especially if the trail records inputs or is based on patterns or time of usage.

Related Controls: AU-2, AU-8, AU-12, MA-4, SA-8, SI-7, SI-11.

Control Enhancements:

(1) CONTENT OF AUDIT RECORDS | ADDITIONAL AUDIT INFORMATION

[Existing] [Priority 2]

Control:

Generate audit records containing the following additional information:

- a. Session, connection, transaction, and activity duration;
- b. Source and destination addresses;
- c. Object or filename involved; and
- d. Number of bytes received and bytes sent (for client-server transactions) in the audit records for audit events identified by type, location, or subject.
- e. The III portion of the log shall clearly identify:
 1. The operator
 2. The authorized receiving agency
 3. The requestor
 4. The secondary recipient

Discussion: The ability to add information generated in audit records is dependent on system functionality to configure the audit record content. Organizations may consider additional information in audit records including, but not limited to, access control or flow control rules invoked and individual identities of group account users. Organizations may also consider limiting additional audit record information to only information that is explicitly needed for audit requirements. This facilitates the use of audit trails and audit logs by not including information in audit records that could potentially be misleading, make it more difficult to locate information of interest, or increase the risk to individuals' privacy.

Related Controls: None.

(3) CONTENT OF AUDIT RECORDS | LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS

[Priority 2]

Control:

Limit personally identifiable information contained in audit records to the following elements identified in the privacy risk assessment: minimum PII necessary to achieve the purpose for which it is collected (see Section 4.3).

Discussion: Limiting personally identifiable information in audit records when such information is not needed for operational purposes helps reduce the level of privacy risk created by a system.

Related Controls: RA-3.

AU-4 AUDIT LOG STORAGE CAPACITY

[Priority 2]

Control:

Allocate audit log storage capacity to accommodate the collection of audit logs to meet retention requirements (AU-11).

Discussion: Organizations consider the types of audit logging to be performed and the audit log processing requirements when allocating audit log storage capacity. Allocating sufficient audit log storage capacity reduces the likelihood of such capacity being exceeded and resulting in the potential loss or reduction of audit logging capability.

Related Controls: AU-2, AU-5, AU-6, AU-7, AU-9, AU-11, AU-12, SI-4.

AU-5 RESPONSE TO AUDIT LOGGING PROCESS FAILURES

[Existing] [Priority 2]

Control:

- a. Alert organizational personnel with audit and accountability responsibilities and system/network administrators within one (1) hour in the event of an audit logging process failure; and
- b. Take the following additional actions: restart all audit logging processes and verify system(s) are logging properly.

Discussion: Audit logging process failures include software and hardware errors, failures in audit log capturing mechanisms, and reaching or exceeding audit log storage capacity. Organization- defined actions include overwriting oldest audit records, shutting down the system, and stopping the generation of audit records. Organizations may choose to define additional actions for audit logging process failures based on the type of failure, the location of the failure, the severity of the failure, or a combination of such factors. When the audit logging process failure is related to storage, the response is carried out for the audit log storage repository (i.e., the distinct system component where the audit logs are stored), the system on which the

audit logs reside, the total audit log storage capacity of the organization (i.e., all audit log storage repositories combined), or all three.

Related Controls: AU-2, AU-4, AU-7, AU-9, AU-11, AU-12, SI-4, SI-12.

AU-6 AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING

[Existing] [Priority 2]

Control:

- a. Review and analyze system audit records weekly for indications of inappropriate or unusual activity and the potential impact of the inappropriate or unusual activity;
- b. Report findings to organizational personnel with audit review, analysis, and reporting responsibilities and organizational personnel with information security and privacy responsibilities; and
- c. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.

Discussion: Audit record review, analysis, and reporting covers information security- and privacy- related logging performed by organizations, including logging that results from the monitoring of account usage, remote access, wireless connectivity, mobile device connection, configuration settings, system component inventory, use of maintenance tools and non-local maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at system interfaces, and use of mobile code or Voice over Internet Protocol (VoIP). Findings can be reported to organizational entities that include the incident response team, help desk, and security or privacy offices. If organizations are prohibited from reviewing and analyzing audit records or unable to conduct such activities, the review or analysis may be carried out by other organizations granted such authority. The frequency, scope, and/or depth of the audit record review, analysis, and reporting may be adjusted to meet organizational needs based on new information received.

Related Controls: AC-2, AC-3, AC-5, AC-6, AC-7, AC-17, AU-7, CA-2, CA-7, CM-2, CM-5, CM-6, CM-10, CM-11, IA-2, IA-3, IA-5, IA-8, IR-5, MA-4, MP-4, PE-3, PE-6, RA-5, SA-8, SC-7, SI-3, SI-4, SI-7.

Control Enhancements:

(1) AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING |AUTOMATED PROCESS INTEGRATION

[Priority 2]

Control:

Integrate audit record review, analysis, and reporting processes using automated mechanisms.

Discussion: Organizational processes that benefit from integrated audit record review, analysis, and reporting include incident response, continuous monitoring, contingency planning, investigation and response to suspicious activities, and Inspector General audits.

(3) AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | CORRELATE AUDIT RECORD REPOSITORIES

[Priority 2]

Control:

Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.

Discussion: Organization-wide situational awareness includes awareness across all three levels of risk management (i.e., organizational level, mission/business process level, and information system level) and supports cross-organization awareness.

Related Controls: AU-12, IR-4.

AU-7 AUDIT RECORD REDUCTION AND REPORT GENERATION

[Priority 3]

Control:

Provide and implement an audit record reduction and report generation capability that:

- a. Supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents; and
- b. Does not alter the original content or time ordering of audit records.

Discussion: Audit record reduction is a process that manipulates collected audit log information and organizes it into a summary format that is more meaningful to analysts. Audit record reduction and report generation capabilities do not always emanate from the same system or from the same organizational entities that conduct audit logging activities. The audit record reduction capability includes modern data mining techniques with advanced data filters to identify anomalous behavior in audit records. The report generation capability provided by the system can generate customizable reports. Time ordering of audit records can be an issue if the granularity of the timestamp in the record is insufficient.

Related Controls: AC-2, AU-2, AU-3, AU-4, AU-5, AU-6, AU-12, CM-5, IA-5, IR-4, SI-4.

Control Enhancements:

(1) AUDIT RECORD REDUCTION AND REPORT GENERATION | AUTOMATIC PROCESSING

[Priority 3]

Control:

Provide and implement the capability to process, sort, and search audit records for events of interest based on the following content: information included in AU-3.

Discussion: Events of interest can be identified by the content of audit records, including system resources involved, information objects accessed, identities of individuals, event types, event locations, event dates and times, Internet Protocol addresses involved, or event success or failure. Organizations may define event criteria to any degree of granularity required, such as locations selectable by a general networking location or by specific system component.

AU-8 TIME STAMPS

[Existing] [Priority 2]

Control:

- a. Use internal system clocks to generate time stamps for audit records;
- b. Record time stamps for audit records that meet hundredths of a second (i.e., hh:mm:ss:00) interval and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.

Discussion: Time stamps generated by the system include date and time. Time is commonly expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. Granularity of time measurements refers to the degree of synchronization between system clocks and reference clocks (e.g., clocks synchronizing within hundreds of milliseconds or tens of milliseconds). Organizations may define different time granularities for different system components. Time service can be critical to other security capabilities such as access control and identification and authentication, depending on the nature of the mechanisms used to support those capabilities.

Related Controls: AU-3, AU-12.

AU-9 PROTECTION OF AUDIT INFORMATION

[Existing] [Priority 2]

Control:

- a. Protect audit information and audit logging tools from unauthorized access, modification, and deletion; and
- b. Alert organizational personnel with audit and accountability responsibilities, organizational personnel with information security and privacy responsibilities, and system/network administrators upon detection of unauthorized access, modification, or deletion of audit information.

Discussion: Audit information includes all information needed to successfully audit system activity, such as audit records, audit log settings, audit reports, and personally identifiable information. Audit logging tools are those programs and devices used to conduct system audit and logging activities. Protection of audit information focuses on technical protection and limits

the ability to access and execute audit logging tools to authorized individuals. Physical protection of audit information is addressed by both media protection controls and physical and environmental protection controls.

Related Controls: AC-3, AC-6, AU-6, AU-11, MP-2, MP-4, PE-2, PE-3, PE-6, SA-8, SC-8, SI-4.

Control Enhancements:

(4) PROTECTION OF AUDIT INFORMATION | ACCESS BY SUBSET OF PRIVILEGED USERS

[Priority 2]

Control:

Authorize access to management of audit logging functionality to only organizational personnel with audit and accountability responsibilities, organizational personnel with information security and privacy responsibilities, and system/network administrators.

Discussion: Individuals or roles with privileged access to a system and who are also the subject of an audit by that system may affect the reliability of the audit information by inhibiting audit activities or modifying audit records. Requiring privileged access to be further defined between audit-related privileges and other privileges limits the number of users or roles with audit-related privileges.

Related Controls: AC-5.

AU-11 AUDIT RECORD RETENTION

[Existing] [Priority 4]

Control:

Retain audit records for a minimum of one (1) year or until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.

Discussion: Organizations retain audit records until it is determined that the records are no longer needed for administrative, legal, audit, or other operational purposes. This includes the retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoenas, and law enforcement actions. Organizations develop standard categories of audit records relative to such types of actions and standard response processes for each type of action.

Related Controls: AU-2, AU-4, AU-5, AU-6, AU-9, MP-6, RA-5, SI-12.

AU-12 AUDIT RECORD GENERATION

[Priority 2]

Control:

- a. Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on all systems generating required audit logs;
- b. Allow organizational personnel with audit record generation responsibilities, organizational personnel with information security and privacy responsibilities, and system/network administrators to select the event types that are to be logged by specific components of the system; and
- c. Generate audit records for the event types defined in AU-2c that include the audit record content defined in AU-3.

Discussion: Audit records can be generated from many different system components. The event types specified in AU-2c are the event types for which audit logs are to be generated and are a subset of all event types for which the system can generate audit records.

Related Controls: AC-6, AC-17, AU-2, AU-3, AU-4, AU-5, AU-6, AU-7, CM-5, MA-4, MP-4, SA-8, SC-18, SI-3, SI-4, SI-7, SI-10.

ASSESSMENT, AUTHORIZATION, AND MONITORING (CA)

CA-1 POLICY AND PROCEDURES

[Priority 2]

Control:

- a. Develop, document, and disseminate to organizational personnel with assessment, authorization, and monitoring policy responsibilities:
 1. An assessment, authorization, and monitoring policy that:
 - (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 - (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
 2. Procedures to facilitate the implementation of the assessment, authorization, and monitoring policy and the associated assessment, authorization, and monitoring controls;
- b. Designate organizational personnel with information security responsibilities to manage the development, documentation, and dissemination of the assessment, authorization, and monitoring policy and procedures; and
- c. Review and update the current assessment, authorization, and monitoring:
 1. Policy annually and following changes to the assessment criteria and
 2. Procedures annually and following changes to the assessment criteria.

Discussion: Assessment, authorization, and monitoring policy and procedures address the controls in the CA family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of assessment, authorization, and monitoring policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to assessment, authorization, and monitoring policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PS-8, SI-12.

CA-2 CONTROL ASSESSMENTS

[Priority 3]

Control:

- a. Select the appropriate assessor or assessment team for the type of assessment to be conducted;
- b. Develop a control assessment plan that describes the scope of the assessment including:
 1. Controls and control enhancements under assessment;
 2. Assessment procedures to be used to determine control effectiveness; and
 3. Assessment environment, assessment team, and assessment roles and responsibilities;
- c. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment;
- d. Assess the controls in the system and its environment of operation and any controls that have been impacted by evolving threats at least once every three years to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements;
- e. Produce a control assessment report that documents the results of the assessment; and
- f. Provide the results of the control assessment report to the individual who executed the CJIS User Agreement or is in contract with the FBI.

Discussion: Organizations ensure that control assessors possess the required skills and technical expertise to develop effective assessment plans and to conduct assessments of system-specific, hybrid, common, and program management controls, as appropriate. The required skills include general knowledge of risk management concepts and approaches as well as comprehensive knowledge of and experience with the hardware, software, and firmware system components implemented.

Organizations assess controls in systems and the environments in which those systems operate as part of initial and ongoing authorizations, continuous monitoring, system design and development, systems security engineering, privacy engineering, and the system development life cycle. Assessments help to ensure that organizations meet information security and privacy requirements, identify weaknesses and deficiencies in the system design and development process, provide essential information needed to make risk-based decisions as part of authorization processes, and comply with vulnerability mitigation procedures. Organizations conduct assessments on the implemented controls as documented in security and privacy plans. Assessments can also be conducted throughout the system development life cycle as part of systems engineering and systems security engineering processes. The design for controls can be assessed as RFPs are developed, responses assessed, and design reviews conducted. If a design to implement controls and subsequent implementation in accordance with the design are assessed during development, the final control testing can be a simple confirmation utilizing previously completed control assessment and aggregating the outcomes.

Organizations may develop a single, consolidated security and privacy assessment plan for the system or maintain separate plans. A consolidated assessment plan clearly delineates the roles

and responsibilities for control assessment. If multiple organizations participate in assessing a system, a coordinated approach can reduce redundancies and associated costs.

Organizations can use other types of assessment activities, such as vulnerability scanning and system monitoring, to maintain the security and privacy posture of systems during the system life cycle. Assessment reports document assessment results in sufficient detail, as deemed necessary by organizations, to determine the accuracy and completeness of the reports and whether the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting requirements. Assessment results are provided to the individuals or roles appropriate for the types of assessments being conducted. For example, assessments conducted in support of authorization decisions are provided to authorizing officials, senior agency officials for privacy, senior agency information security officers, and authorizing official designated representatives (i.e., CJIS Systems Officer [CSO], Interface Agency [IA] Official, or FBI Compact Officer [CO]).

To satisfy assessment requirements, organizations can use assessment results from the following sources: initial or ongoing system authorizations, continuous monitoring, systems engineering processes, or system development life cycle activities. Organizations ensure that assessment results are current, relevant to the determination of control effectiveness, and obtained with the appropriate level of assessor independence. Existing control assessment results can be reused to the extent that the results are still valid and can also be supplemented with additional assessments as needed. After the initial authorizations, organizations assess controls during continuous monitoring. Organizations also establish the frequency for ongoing assessments in accordance with organizational continuous monitoring strategies. External audits, including audits by external entities such as regulatory agencies, are outside of the scope of CA-2.

Related Controls: AC-20, CA-5, CA-6, CA-7, RA-5, SA-11, SI-3, SI-12, SR-2, SR-3.

Control Enhancements:

(1) CONTROL ASSESSMENTS | INDEPENDENT ASSESSORS

[Priority 3]

Control:

Employ independent assessors or assessment teams to conduct control assessments.

Discussion: Independent assessors or assessment teams are individuals or groups who conduct impartial assessments of systems. Impartiality means that assessors are free from any perceived or actual conflicts of interest regarding the development, operation, sustainment, or management of the systems under assessment or the determination of control effectiveness. To achieve impartiality, assessors do not create a mutual or conflicting interest with the organizations where the assessments are being conducted, assess their own work, act as management or employees of the organizations they are serving, or place themselves in positions of advocacy for the organizations acquiring their services.

Independent assessments can be obtained from elements within organizations or be contracted to public or private sector entities outside of organizations. Authorizing officials determine the required level of independence based on the security categories of systems and/or the risk to organizational operations, organizational assets, or individuals. Authorizing officials also determine if the level of assessor independence provides sufficient assurance that the results are

sound and can be used to make credible, risk-based decisions. Assessor independence determination includes whether contracted assessment services have sufficient independence, such as when system owners are not directly involved in contracting processes or cannot influence the impartiality of the assessors conducting the assessments. During the system design and development phase, having independent assessors is analogous to having independent SMEs involved in design reviews.

When organizations that own the systems are small or the structures of the organizations require that assessments be conducted by individuals that are in the developmental, operational, or management chain of the system owners, independence in assessment processes can be achieved by ensuring that assessment results are carefully reviewed and analyzed by independent teams of experts to validate the completeness, accuracy, integrity, and reliability of the results.

Assessments performed for purposes other than to support authorization decisions are more likely to be useable for such decisions when performed by assessors with sufficient independence, thereby reducing the need to repeat assessments.

Related Controls: None.

CA-3 INFORMATION EXCHANGE

[Existing] [Priority 2]

Control:

- a. Approve and manage the exchange of information between the agency system and external systems using the following agreements when applicable;
 1. Executed CJIS User Agreements
 - a. Each CSA, SIB, or IA shall execute a signed written agreement (see Appendix D.1) with the FBI CJIS Division stating their willingness to demonstrate conformity with the CJISSECPOL before accessing and consuming CJIS systems and services as set forth in the agreement.
 - b. The agreement shall include the standards, audit, and sanctions governing utilization of CJIS systems and services.
 - c. The FBI CJIS Division is authorized to periodically test the ability to penetrate the FBI's network through the external connection or system upon proper notification of all signatories in the user agreement.
 2. Criminal Justice Agency User Agreements
 - a. Any CJA receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA providing the access.
 - b. The written agreement shall specify the FBI CJIS systems and services to which the agency will have access, and the FBI CJIS Division policies to which the agency must adhere. These agreements shall include:
 - i. Audit
 - ii. Dissemination
 - iii. Hit confirmation
 - iv. Logging

- v. Quality Assurance (QA)
- vi. Screening (Criminal Justice Employment)
- vii. Security
- viii. Timeliness
- ix. Training
- x. Use of the system
- xi. Validation

3. Agreements for Noncriminal Justice Use of CHRI

A CJA, NCJA (public), or NCJA (private) designated to request civil fingerprint-based background checks, with full consent of the individual to whom the background check is taking place, for noncriminal justice functions, shall be eligible for access to CHRI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. The CJA, NCJA (public), or NCJA (private) receiving access to CHRI shall enter into signed written agreements with the appropriate signatory authority of the CSA, SIB, or authorized agency providing the access. The written agreement shall specify the policies to which the agency must adhere, which includes all pertinent areas of the CJISSECPOL. Each NCJA that directly access FBI systems shall allow the FBI to periodically test the ability to penetrate the FBI's network through the external connection or system. A CJA, NCJA (public), or NCJA (private) authorized to access CHRI for noncriminal justice functions pursuant to federal law or state statute approved by the U.S. Attorney General (defined by the Compact Council as an Authorized Recipient), cannot make CHRI available to another governmental agency, nongovernmental agency, or private contractor to perform noncriminal justice administrative functions without implementation of one of the following:

- a. Security and Management Control Outsourcing Standard for Non-Channelers. Implementation is applicable to noncriminal justice administrative functions that do not require a direct connection to the FBI for submission of fingerprints and receipt of CHRI. Examples include making fitness determinations, processing, storing, or destroying documents, and maintaining IT platforms that do not connect to CJIS systems. Prior to implementation, Authorized Recipients must request and receive written permission from the State Compact Officer, Chief Administrator of the state's criminal history record repository, or the FBI Compact Officer, as applicable.
- b. Security and Management Control Outsourcing Standard for Channeling. Implementation is applicable only to Channeling functions performed by an FBI-approved Channeler that require a direct connection to the FBI for submission of fingerprints and receipt of CHRI. Prior to implementation, Authorized Recipients must request and receive written permission from the State Compact Officer, Chief Administrator of the state's criminal history record repository, or the FBI Compact Officer, as applicable.
- c. Management Control Agreement or Security Addendum (see Appendix H) pursuant to Title 28, C.F.R., Section 20.33 (a) (6) or (7). Although by regulation

implementation of a Management Control Agreement or the Security Addendum is applicable to the administration of criminal justice pursuant to that agreement performed on behalf of CJAs, under very limited circumstances, implementation may also be applicable to CJAs that obtain and use CHRI for noncriminal justice purposes. Implementation for noncriminal justice purposes is only applicable when another governmental agency or private contractor performs both criminal justice and noncriminal justice administrative functions involving access to CHRI on behalf of the CJA. It is important to note that if the servicing governmental agency or private contractor solely performs noncriminal justice administrative functions, then the CJA would be required to implement the Security and Management Control Outsourcing Standard for Non-Channelers.

- b. Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated; and
- c. Review and update the agreements at least triennially or when responsibilities or signatories change.
- d. Secondary Dissemination
 - 1. Log the dissemination of CHRI when released to another authorized agency, and that agency was not part of the releasing agency's primary information exchange agreement(s). If CJI does not contain CHRI and is not part of an information exchange agreement, then it does not need to be logged.
 - 2. Validate the requestor of CJI in conformance with the local policy as an employee and/or contractor of a law enforcement agency or civil agency requiring the CJI to perform their mission; or a member of the public receiving CJI via authorized dissemination.

Discussion: System information exchange requirements apply to information exchanges between two or more systems. System information exchanges include connections via leased lines or virtual private networks, connections to internet service providers, database sharing or exchanges of database transaction information, connections and exchanges with cloud services, exchanges via web-based services, or exchanges of files via file transfer protocols, network protocols (e.g., IPv4, IPv6), email, or other organization-to-organization communications. Organizations consider the risk related to new or increased threats that may be introduced when systems exchange information with other systems that may have different security and privacy requirements and controls. This includes systems within the same organization and systems that are external to the organization. An example of an NCJA (public) is a county school board. An example of an NCJA (private) is a local bank.

Authorizing officials determine the risk associated with system information exchange and the controls needed for appropriate risk mitigation. The types of agreements selected are based on factors such as the impact level of the information being exchanged, the relationship between the organizations exchanging information (e.g., government to government, government to business, business to business, government or business to service provider, government or business to individual), or the level of access to the organizational system by users of the other system. If systems that exchange information have the same authorizing official, organizations need not develop agreements. Instead, the interface characteristics between the systems (e.g., how the information is being exchanged, how the information is protected) are described in the respective

security and privacy plans. If the systems that exchange information have different authorizing officials within the same organization, the organizations can develop agreements or provide the same information that would be provided in the appropriate agreement type from CA-3a in the respective security and privacy plans for the systems. Organizations may incorporate agreement information into formal contracts, especially for information exchanges established between federal agencies and nonfederal organizations (including service providers, contractors, system developers, and system integrators). Risk considerations include systems that share the same networks.

Related Controls: AC-4, AC-20, CA-6, IA-3, IR-4, PL-2, RA-3, SA-9, SC-7, SI-12.

CA-5 PLAN OF ACTION AND MILESTONES

[Priority 4]

Control:

- a. Develop a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and
- b. Update existing plan of action and milestones at least every six (6) months or when new information is available based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.

Discussion: Plans of action and milestones are useful for any type of organization to track planned remedial actions. Related Controls: CA-2, CA-7, RA-7, SI-2, SI-12.

CA-6 AUTHORIZATION

[Priority 3]

Control:

- a. Assign a senior official as the responsible official for the system;
- b. Assign the CSO, SIB Chief, or IA Official as the authorizing official for common controls available for inheritance by organizational systems;
- c. Ensure that the authorizing official for the system, before commencing operations:
 1. Accepts the use of common controls inherited by the system; and
 2. Authorizes the system to operate;
- d. Ensure that the authorizing official for common controls authorizes the use of those controls for inheritance by organizational systems;
- e. Update the authorizations at least every three (3) years.

Discussion: Authorizations are official management decisions by senior officials to authorize operation of systems, authorize the use of common controls for inheritance by organizational systems, and explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of agreed-upon controls. Authorizing

officials provide budgetary oversight for organizational systems and common controls or assume responsibility for the mission and business functions supported by those systems or common controls. Authorizing officials are both responsible and accountable for security and privacy risks associated with the operation and use of organizational systems.

Nonfederal organizations may have similar processes to authorize systems and senior officials that assume the authorization role and associated responsibilities.

Authorizing officials issue ongoing authorizations of systems based on evidence produced from implemented continuous monitoring programs. Robust continuous monitoring programs reduce the need for separate reauthorization processes. Through the employment of comprehensive continuous monitoring processes, the information contained in authorization packages (i.e., security and privacy plans, assessment reports, and plans of action and milestones) is updated on an ongoing basis. This provides authorizing officials, common control providers, and system owners with an up-to-date status of the security and privacy posture of their systems, controls, and operating environments. To reduce the cost of reauthorization, authorizing officials can leverage the results of continuous monitoring processes to the maximum extent possible as the basis for rendering reauthorization decisions.

Related Controls: CA-2, CA-3, CA-7, RA-3, SA-10, SI-12.

CA-7 CONTINUOUS MONITORING

[Priority 1]

Control:

Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes:

a. Establishing the following system-level metrics to be monitored:

1. AC-2(g) Account Management
2. AC-17(1) Remote Access | Monitoring and Control
3. AT-4(a) Training Records
4. CM-3(f) Configuration Change Control
5. CM-6(d) Configuration Settings
6. CM-11(c) User-Installed Software
7. IR-5 Incident Monitoring
8. MA-2(b) Controlled Maintenance
9. MA-3(a) Maintenance Tool
10. MA-4(a) Nonlocal Maintenance
11. PE-3(d) Physical Access Control
12. PE-6 Monitoring Physical Access
13. PE-14(b) Environmental Controls

- 14. PE-16 Delivery and Removal
- 15. PS-7(e) External Personnel Security
- 16. SA-9(c) External System Services
- 17. SC-7(a) Boundary Protection
- 18. SC-7(24)(b) Boundary Protection | Personally Identifiable Information
- 19. SC-18(b) Mobile Code
- 20. SI-4 System Monitoring

- b. Establishing an ongoing frequency for monitoring and an ongoing frequency for assessment of control effectiveness;
- c. Ongoing control assessments in accordance with the continuous monitoring strategy;
- d. Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy;
- e. Correlation and analysis of information generated by control assessments and monitoring;
- f. Response actions to address results of the analysis of control assessment and monitoring information; and
- g. Reporting the security and privacy status of the system to organizational personnel with information security, privacy responsibilities, and system/network administrators annually, when security events/incidents occur, and when requested.

Discussion: Continuous monitoring at the system level facilitates ongoing awareness of the system security and privacy posture to support organizational risk management decisions. The terms “continuous” and “ongoing” imply that organizations assess and monitor their controls and risks at a frequency sufficient to support risk-based decisions. Different types of controls may require different monitoring frequencies. The results of continuous monitoring generate risk response actions by organizations. When monitoring the effectiveness of multiple controls that have been grouped into capabilities, a root-cause analysis may be needed to determine the specific control that has failed. Continuous monitoring programs allow organizations to maintain the authorizations of systems and common controls in highly dynamic environments of operation with changing mission and business needs, threats, vulnerabilities, and technologies. Having access to security and privacy information on a continuing basis through reports and dashboards gives organizational officials the ability to make effective and timely risk management decisions, including ongoing authorization decisions.

Automation supports more frequent updates to hardware, software, and firmware inventories, authorization packages, and other system information. Effectiveness is further enhanced when continuous monitoring outputs are formatted to provide information that is specific, measurable, actionable, relevant, and timely. Continuous monitoring activities are scaled in accordance with the security categories of systems. Monitoring requirements, including the need for specific monitoring, may be referenced in other controls and control enhancements.

Related Controls: AC-2, AC-6, AC-17, AT-4, AU-6, CA-2, CA-5, CA-6, CM-3, CM-4, CM-6, CM-11, IA-5, IR-5, MA-2, MA-3, MA-4, PE-3, PE-6, PE-14, PE-16, PL-2, PS-7, RA-3, RA-5, RA-7, SA-8, SA-9, SA-11, SC-5, SC-7, SC-18, SI-3, SI-4, SI-12, SR-6.

Control Enhancements:

(1) CONTINUOUS MONITORING | INDEPENDENT ASSESSMENT

[Priority 1]

Control:

Employ independent assessors or assessment teams to monitor the controls in the system on an ongoing basis.

Discussion: Organizations maximize the value of control assessments by requiring that assessments be conducted by assessors with appropriate levels of independence. The level of required independence is based on organizational continuous monitoring strategies.

Assessor independence provides a degree of impartiality to the monitoring process. To achieve such impartiality, assessors do not create a mutual or conflicting interest with the organizations where the assessments are being conducted, assess their own work, act as management or employees of the organizations they are serving, or place themselves in advocacy positions for the organizations acquiring their services.

Related Controls: None.

(4) CONTINUOUS MONITORING | RISK MONITORING

[Priority 1]

Control:

Ensure risk monitoring is an integral part of the continuous monitoring strategy that includes the following:

- a. Effectiveness monitoring;
- b. Compliance monitoring; and
- c. Change monitoring.

Discussion: Risk monitoring is informed by the established organizational risk tolerance. Effectiveness monitoring determines the ongoing effectiveness of the implemented risk response measures. Compliance monitoring verifies that required risk response measures are implemented. It also verifies that security and privacy requirements are satisfied. Change monitoring identifies changes to organizational systems and environments of operation that may affect security and privacy risk.

Related Controls: None.

CA-9 INTERNAL SYSTEM CONNECTIONS

[Priority 3]

Control:

- a. Authorize internal connections of components with the capability to process, store, or transmit CJI to the system;
- b. Document, for each internal connection, the interface characteristics, security and privacy

requirements, and the nature of the information communicated;

- c. Terminate internal system connections when no longer required or authorized; and
- d. Review at least annually the continued need for each internal connection.

Discussion: Internal system connections are connections between organizational systems and separate constituent system components (i.e., connections between components that are part of the same system) including components used for system development. Intra-system connections include connections with mobile devices, notebook and desktop computers, tablets, printers, copiers, facsimile machines, scanners, sensors, and servers. Instead of authorizing each internal system connection individually, organizations can authorize internal connections for a class of system components with common characteristics and/or configurations, including printers, scanners, and copiers with a specified processing, transmission, and storage capability or smart phones and tablets with a specific baseline configuration. The continued need for an internal system connection is reviewed from the perspective of whether it provides support for organizational missions or business functions.

Related Controls: AC-3, AC-4, AC-18, AC-19, CM-2, IA-3, SC-7, SI-12.

CONFIGURATION MANAGEMENT (CM)

CM-1 POLICY AND PROCEDURES

[Priority 2]

Control:

- a. Develop, document, and disseminate to organizational personnel with configuration management responsibilities:
 1. Agency-level configuration management policy that:
 - (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 - (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
 2. Procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls;
- b. Designate organizational personnel with information security responsibilities to manage the development, documentation, and dissemination of the configuration management policy and procedures; and
- c. Review and update the current configuration management:
 1. Policy annually and following any hardware or software changes to systems which process, store, or transmit CJI; and
 2. Procedures annually and following any hardware or software changes to systems which process, store, or transmit CJI.

Discussion: Configuration management policy and procedures address the controls in the CM family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of configuration management policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission/business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to configuration management policy and procedures include, but are not limited to, assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PS-8, SA-8, SI-12.

CM-2 BASELINE CONFIGURATION

[Existing] [Priority 1]

Control:

- a. Develop, document, and maintain under configuration control, a current baseline configuration of the system;
- b. Develop, document, and maintain a current and complete topological drawing depicting the interconnectivity of the agency network to criminal justice information systems and services; and
- c. Review and update the baseline configuration and topological drawing of the system:
 1. At least annually;
 2. When required due to security-relevant changes to the system and/or security incidents occur; and
 3. When system components are installed or upgraded.

Discussion: Baseline configurations for systems and system components include connectivity, operational, and communications aspects of systems. Baseline configurations are documented, formally reviewed, and agreed-upon specifications for systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, or changes to systems and include security and privacy control implementations, operational procedures, information about system components, network topology, and logical placement of components in the system architecture. Maintaining baseline configurations requires creating new baselines as organizational systems change over time. Baseline configurations of systems reflect the current enterprise architecture. See Appendix C for sample topological/network diagrams.

Related Controls: AC-19, AU-6, CA-9, CM-1, CM-3, CM-5, CM-6, CM-8, CM-9, CP-9, CP-10, MA-2, PL-8, SA-8, SA-10, SA-15, SC-18.

Control Enhancements:

(2) BASELINE CONFIGURATION | AUTOMATION SUPPORT FOR ACCURACY AND CURRENCY

[Priority 1]

Control:

Maintain the currency, completeness, accuracy, and availability of the baseline configuration of the system using automated mechanisms such as configuration management tools, hardware, software, firmware inventory tools, and network management tools.

Discussion: Automated mechanisms that help organizations maintain consistent baseline configurations for systems include configuration management tools, hardware, software, firmware inventory tools, and network management tools. Automated tools can be used at the

organization level, mission and business process level, or system level on workstations, servers, notebook computers, network components, or mobile devices. Tools can be used to track version numbers on operating systems, applications, types of software installed, and current patch levels. Automation support for accuracy and currency can be satisfied by the implementation of CM-8(2) for organizations that combine system component inventory and baseline configuration activities.

Related Controls: CM-7, IA-3, RA-5.

(3) BASELINE CONFIGURATION | RETENTION OF PREVIOUS CONFIGURATIONS

[Priority 1]

Control:

Retain at least one (1) previous version of baseline configurations of the system to support rollback.

Discussion: Retaining previous versions of baseline configurations to support rollback include hardware, software, firmware, configuration files, configuration records, and associated documentation.

Related Controls: None.

(7) BASELINE CONFIGURATION | CONFIGURE SYSTEMS AND COMPONENTS FOR HIGH-RISK AREAS

[Existing] [Priority 1]

Control:

- a. Issue devices (e.g., mobile devices) with CJISSECPOL compliant configurations to individuals traveling to locations that the organization deems to be of significant risk; and
- b. Apply the following controls to the systems or components when the individuals return from travel: examine the device for signs of physical tampering, purge and reimage disk drives and/or devices as required, and ensure all security controls are in place and functional.

Discussion: When it is known that systems or system components will be in high-risk areas external to the organization, additional controls may be implemented to counter the increased threat in such areas. For example, organizations can take actions for notebook computers used by individuals departing on and returning from travel. Actions include determining the locations that are of concern, defining the required configurations for the components, ensuring that components are configured as intended before travel is initiated, and applying controls to the components after travel is completed. Specially configured notebook computers include computers with sanitized hard drives, limited applications, and more stringent configuration settings. Controls applied to mobile devices upon return from travel include examining the mobile device for signs of physical tampering and purging and reimaging disk drives. Protecting information that resides on mobile devices is addressed in the MP (Media Protection) family.

Related Controls: MP-4, MP-5.

CM-3 CONFIGURATION CHANGE CONTROL

[Priority 2]

Control:

- a. Determine and document the types of changes to the system that are configuration-controlled;
- b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses;
- c. Document configuration change decisions associated with the system;
- d. Implement approved configuration-controlled changes to the system;
- e. Retain records of configuration-controlled changes to the system for two (2) years;
- f. Monitor and review activities associated with configuration-controlled changes to the system; and
- g. Coordinate and provide oversight for configuration change control activities through personnel with configuration management responsibilities, a Configuration Control Board, or Change Advisory Board that convenes regularly or when hardware or software changes (i.e., updates, upgrades, replacements, etc.) to the information system are required.

Discussion: Configuration change control for organizational systems involves the systematic proposal, justification, implementation, testing, review, and disposition of system changes, including system upgrades and modifications. Configuration change control includes changes to baseline configurations, configuration items of systems, operational procedures, configuration settings for system components, remediate vulnerabilities, and unscheduled or unauthorized changes. Processes for managing configuration changes to systems include Configuration Control Boards or Change Advisory Boards that review and approve proposed changes. For changes that impact privacy risk, the senior agency official for privacy updates privacy impact assessments and system of records notices. For new systems or major upgrades, organizations consider including representatives from the development organizations on the Configuration Control Boards or Change Advisory Boards. Auditing of changes includes activities before and after changes are made to systems and the auditing activities required to implement such changes. See also SA-10.

Related Controls: CA-7, CM-2, CM-4, CM-5, CM-6, CM-9, CM-11, IA-3, MA-2, PE-16, SA-8, SA-10, SC-28, SI-2, SI-3, SI-4, SI-7, SI-10, SR-11.

Control Enhancements:

(2) CONFIGURATION CHANGE CONTROL | TESTING, VALIDATION, AND DOCUMENTATION OF CHANGES

[Priority 2]

Control:

Test, validate, and document changes to the system before finalizing the implementation of the changes.

Discussion: Changes to systems include modifications to hardware, software, or firmware

components and configuration settings defined in CM-6. Organizations ensure that testing does not interfere with system operations that support organizational mission and business functions. Individuals or groups conducting tests understand security and privacy policies and procedures, system security and privacy policies and procedures, and the health, safety, and environmental risks associated with specific facilities or processes. Operational systems may need to be taken offline, or replicated to the extent feasible, before testing can be conducted. If systems must be taken offline for testing, the tests are scheduled to occur during planned system outages whenever possible. If the testing cannot be conducted on operational systems, organizations employ compensating controls.

Related Controls: None.

(4) CONFIGURATION CHANGE CONTROL | SECURITY AND PRIVACY REPRESENTATIVES

[Priority 2]

Control:

Require organizational personnel with information security and privacy responsibilities to be members of the Configuration Control Board or Change Advisory Board.

Discussion: Information security and privacy representatives include system security officers, senior agency information security officers, senior agency officials for privacy, or system privacy officers. Representation by personnel with information security and privacy expertise is important because changes to system configurations can have unintended side effects, some of which may be security- or privacy-relevant. Detecting such changes early in the process can help avoid unintended, negative consequences that could ultimately affect the security and privacy posture of systems. The configuration change control element referred to in the second organization-defined parameter reflects the change control elements defined by organizations in CM-3g.

CM-4 IMPACT ANALYSES

[Priority 3]

Control:

Analyze changes to the system to determine potential security and privacy impacts prior to change implementation.

Discussion: Organizational personnel with security or privacy responsibilities conduct impact analyses. Individuals conducting impact analyses possess the necessary skills and technical expertise to analyze the changes to systems as well as the security or privacy ramifications. Impact analyses include reviewing security and privacy plans, policies, and procedures to understand control requirements; reviewing system design documentation and operational procedures to understand control implementation and how specific system changes might affect the controls; reviewing the impact of changes on organizational supply chain partners with stakeholders; and determining how potential changes to a system create new risks to the privacy of individuals and the ability of implemented controls to mitigate those risks. Impact analyses

also include risk assessments to understand the impact of the changes and determine if additional controls are required.

Related Controls: CA-7, CM-3, CM-8, CM-9, MA-2, RA-3, RA-5, SA-5, SA-8, SA-10, SI-2.

Control Enhancements:

(2) IMPACT ANALYSES | VERIFICATION OF CONTROLS

[Priority 3]

Control:

After-system changes, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security and privacy requirements for the system.

Discussion: Implementation in this context refers to installing changed code in the operational system that may have an impact on security or privacy controls.

Related Controls: SA-11.

CM-5 ACCESS RESTRICTIONS FOR CHANGE

[Existing] [Priority 1]

Control:

Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.

Discussion: Changes to the hardware, software, or firmware components of systems or the operational procedures related to the system can potentially have significant effects on the security of the systems or individuals' privacy. Therefore, organizations permit only qualified and authorized individuals to access systems for purposes of initiating changes. Access restrictions include physical and logical access controls (see AC-3 and PE-3), software libraries, workflow automation, media libraries, abstract layers (i.e., changes implemented into external interfaces rather than directly into systems), and change windows (i.e., changes occur only during specified times).

Related Controls: AC-3, AC-5, AC-6, CM-9, PE-3, SC-28, SI-2, SI-10.

CM-6 CONFIGURATION SETTINGS

[Priority 1]

Control:

- a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using established best practices and guidelines such as Defense Information Systems Agency (DISA) Secure Technical Implementation Guidelines (STIGs), Center for Internet Security (CIS) Benchmarks, or Federal Information Processing Standards;

- b. Implement the configuration settings;
- c. Identify, document, and approve any deviations from established configuration settings for system components that store, process, or transmit CJI based on operational requirements; and
- d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

Discussion: Configuration settings are the parameters that can be changed in the hardware, software, or firmware components of the system that affect the security and privacy posture or functionality of the system. Information technology products for which configuration settings can be defined include mainframe computers, servers, workstations, operating systems, mobile devices, input/output devices, protocols, and applications. Parameters that impact the security posture of systems include registry settings; account, file, or directory permission settings; and settings for functions, protocols, ports, services, and remote connections. Privacy parameters are parameters impacting the privacy posture of systems, including the parameters required to satisfy other privacy controls. Privacy parameters include settings for access controls, data processing preferences, and processing and retention permissions. Organizations establish organization-wide configuration settings and subsequently derive specific configuration settings for systems. The established settings become part of the configuration baseline for the system.

Common secure configurations (also known as security configuration checklists, lockdown and hardening guides, and security reference guides) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for information technology products and platforms as well as instructions for configuring those products or platforms to meet operational requirements. Common secure configurations can be developed by a variety of organizations, including information technology product developers, manufacturers, vendors, federal agencies, consortia, academia, industry, and other organizations in the public and private sectors.

Implementation of a common secure configuration may be mandated at the organization level, mission and business process level, system level, or at a higher level, including by a regulatory agency. Common secure configurations include the United States Government Configuration Baseline [USGCB] and security technical implementation guides (STIGs), which affect the implementation of CM-6 and other controls such as AC-19 and CM-7. The Security Content Automation Protocol (SCAP) and the defined standards within the protocol provide an effective method to uniquely identify, track, and control configuration settings.

Related Controls: AC-3, AC-19, AU-2, AU-6, CA-9, CM-2, CM-3, CM-5, CM-7, CM-11, CP-7, CP-9, CP-10, IA-3, IA-5, PL-8, RA-5, SA-4, SA-5, SA-8, SA-9, SC-18, SC-28, SI-2, SI-4.

CM-7 LEAST FUNCTIONALITY

[Existing] [Priority 1]

Control:

- a. Configure the system to provide only essential capabilities to meet operational requirements; and

- b. Prohibit or restrict the use of specified functions, ports, protocols, software, and/or services which are not required.

Discussion: Systems provide a wide variety of functions and services. Some of the functions and services routinely provided by default may not be necessary to support essential organizational missions, functions, or operations. Additionally, it is sometimes convenient to provide multiple services from a single system component, but doing so increases risk over limiting the services provided by that single component. Where feasible, organizations limit component functionality to a single function per component. Organizations consider removing unused or unnecessary software and disabling unused or unnecessary physical and logical ports and protocols to prevent unauthorized connection of components, transfer of information, and tunneling. Organizations employ network scanning tools, intrusion detection and prevention systems, and end-point protection technologies, such as firewalls and host-based intrusion detection systems, to identify and prevent the use of prohibited functions, protocols, ports, and services. Least functionality can also be achieved as part of the fundamental design and development of the system (see SA- 8 and SC-2).

Related Controls: AC-3, AC-4, CM-2, CM-5, CM-6, CM-11, RA-5, SA-4, SA-5, SA-8, SA-9, SA-15, SC- 2, SC-7, SI-4.

Control Enhancements:

(1) LEAST FUNCTIONALITY | PERIODIC REVIEW

[Existing] [Priority 1]

Control:

- a. Review the system annually, as the system changes, or incidents occur to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services; and
- b. Disable or remove functions, ports, protocols, software, and/or services within the system deemed to be unnecessary and/or unsecure.

Discussion: Organizations review functions, ports, protocols, and services provided by systems or system components to determine the functions and services that are candidates for elimination. Such reviews are especially important during transition periods from older technologies to newer technologies (e.g., transition from IPv4 to IPv6). These technology transitions may require implementing the older and newer technologies simultaneously during the transition period and returning to minimum essential functions, ports, protocols, and services at the earliest opportunity. Organizations can either decide the relative security of the function, port, protocol, and/or service or base the security decision on the assessment of other entities. Unsecure protocols include Bluetooth, FTP, and peer-to-peer networking.

Related Controls: AC-18.

(2) LEAST FUNCTIONALITY | PREVENT PROGRAM EXECUTION

[Priority 1]

Control:

Prevent program execution in accordance with rules of behavior and/or rules authorizing the

terms and conditions of software program usage.

Discussion: Prevention of program execution addresses organizational policies, rules of behavior, and/or access agreements that restrict software usage and the terms and conditions imposed by the developer or manufacturer, including software licensing and copyrights. Restrictions include prohibiting auto-execute features, restricting roles allowed to approve program execution, permitting or prohibiting specific software programs, or restricting the number of program instances executed at the same time.

Related Controls: CM-8, PL-4, PS-6.

(5) LEAST FUNCTIONALITY | AUTHORIZED SOFTWARE — ALLOW-BY-EXCEPTION

[Priority 1]

Control:

- a. Identify software programs authorized to execute on the system;
- b. Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system; and
- c. Review and update the list of authorized software programs annually.

Discussion: Authorized software programs can be limited to specific versions or from a specific source. To facilitate a comprehensive authorized software process and increase the strength of protection for attacks that bypass application level authorized software, software programs may be decomposed into and monitored at different levels of detail. These levels include applications, application programming interfaces, application modules, scripts, system processes, system services, kernel functions, registries, drivers, and dynamic link libraries. The concept of permitting the execution of authorized software may also be applied to user actions, system ports and protocols, IP addresses/ranges, websites, and MAC addresses. Organizations consider verifying the integrity of authorized software programs using digital signatures, cryptographic checksums, or hash functions. Verification of authorized software can occur either prior to execution or at system startup. The identification of authorized URLs for websites is addressed in SC-7.

Related Controls: CM-2, CM-6, CM-8, CM-10, SA-10, SI-7.

CM-8 SYSTEM COMPONENT INVENTORY

[Priority 1]

Control:

- a. Develop and document an inventory of system components that:
 1. Accurately reflects the system;
 2. Includes all components within the system;
 3. Does not include duplicate accounting of components or components assigned to any other system;

4. Is at the level of granularity deemed necessary for tracking and reporting; and
5. Includes the following minimum information to achieve system component accountability: date of installation, model, serial number, manufacturer, supplier information, component type, software owner, software version number, software license information, and hardware and physical location; and

b. Review and update the system component inventory annually.

Discussion: System components are discrete, identifiable information technology assets that include hardware, software, and firmware. Organizations may choose to implement centralized system component inventories that include components from all organizational systems. In such situations, organizations ensure that the inventories include system-specific information required for component accountability. The information necessary for effective accountability of system components includes the system name, software owners, software version numbers, hardware inventory specifications, software license information, and for networked components, the machine names and network addresses across all implemented protocols (e.g., IPv4, IPv6). Inventory specifications include date of receipt, cost, model, serial number, manufacturer, supplier information, component type, and physical location.

Preventing duplicate accounting of system components addresses the lack of accountability that occurs when component ownership and system association is not known, especially in large or complex connected systems. Effective prevention of duplicate accounting of system components necessitates use of a unique identifier for each component. For software inventory, centrally managed software that is accessed via other systems is addressed as a component of the system on which it is installed and managed. Software installed on multiple organizational systems and managed at the system level is addressed for each individual system and may appear more than once in a centralized component inventory, necessitating a system association for each software instance in the centralized inventory to avoid duplicate accounting of components. Scanning systems implementing multiple network protocols (e.g., IPv4 and IPv6) can result in duplicate components being identified in different address spaces.

Related Controls: CM-2, CM-7, CM-9, CM-10, CM-11, CP-2, CP-9, MA-2, MA-6, SA-4, SA-5, SI-2.

Control Enhancements:

(1) SYSTEM COMPONENT INVENTORY | UPDATES DURING INSTALLATION AND REMOVAL

[Priority 1]

Control:

Update the inventory of system components as part of component installations, removals, and system updates.

Discussion: Organizations can improve the accuracy, completeness, and consistency of system component inventories if the inventories are updated as part of component installations or removals or during general system updates. If inventories are not updated at these key times, there is a greater likelihood that the information will not be appropriately captured and

documented. System updates include hardware, software, and firmware components.

Related Controls: None.

(3) SYSTEM COMPONENT INVENTORY | AUTOMATED UNAUTHORIZED COMPONENT DETECTION

[Priority 1]

Control:

- a. Detect the presence of unauthorized hardware, software, and firmware components within the system using automated mechanisms continuously or at least weekly; and
- b. Take the following actions when unauthorized components are detected: disable or isolate the unauthorized components and notify organizational personnel with security responsibilities.

Discussion: Automated unauthorized component detection is applied in addition to the monitoring for unauthorized remote connections and mobile devices. Monitoring for unauthorized system components may be accomplished on an ongoing basis or by the periodic scanning of systems for that purpose. Automated mechanisms may also be used to prevent the connection of unauthorized components. Automated mechanisms can be implemented in systems or in separate system components. When acquiring and implementing automated mechanisms, organizations consider whether such mechanisms depend on the ability of the system component to support an agent or supplicant in order to be detected since some types of components do not have or cannot support agents (e.g., IoT devices, sensors). Isolation can be achieved, for example, by placing unauthorized system components in separate domains or subnets or quarantining such components. This type of component isolation is commonly referred to as “sandboxing.”

Related Controls: AC-19, CA-7, RA-5, SC-3, SC-39, SI-3, SI-4, SI-7.

CM-9 CONFIGURATION MANAGEMENT PLAN

[Priority 2]

Control:

Develop, document, and implement a configuration management plan for the system that:

- a. Addresses roles, responsibilities, and configuration management processes and procedures;
- b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;
- c. Defines the configuration items for the system and places the configuration items under configuration management;
- d. Is reviewed and approved by organizational personnel with information security responsibilities and organizational personnel with configuration management responsibilities; and
- e. Protects the configuration management plan from unauthorized disclosure and modification.

Discussion: Configuration management activities occur throughout the system development life cycle. As such, there are developmental configuration management activities (e.g., the control of code and software libraries) and operational configuration management activities (e.g., control of installed components and how the components are configured). Configuration management plans satisfy the requirements in configuration management policies while being tailored to individual systems. Configuration management plans define processes and procedures for how configuration management is used to support system development life cycle activities.

Configuration management plans are generated during the development and acquisition stage of the system development life cycle. The plans describe how to advance changes through change management processes; update configuration settings and baselines; maintain component inventories; control development, test, and operational environments; and develop, release, and update key documents.

Organizations can employ templates to help ensure the consistent and timely development and implementation of configuration management plans. Templates can represent a configuration management plan for the organization with subsets of the plan implemented on a system by system basis. Configuration management approval processes include the designation of key stakeholders responsible for reviewing and approving proposed changes to systems, and personnel who conduct security and privacy impact analyses prior to the implementation of changes to the systems. Configuration items are the system components, such as the hardware, software, firmware, and documentation to be configuration managed. As systems continue through the system development life cycle, new configuration items may be identified, and some existing configuration items may no longer need to be under configuration control.

Related Controls: CM-2, CM-3, CM-4, CM-5, CM-8, PL-2, SA-10, SI-12.

CM-10 SOFTWARE USAGE RESTRICTIONS

[Priority 3]

Control:

- a. Use software and associated documentation in accordance with contract agreements and copyright laws;
- b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and
- c. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

Discussion: Software license tracking can be accomplished by manual or automated methods, depending on organizational needs. Examples of contract agreements include software license agreements and non-disclosure agreements.

Related Controls: AC-17, AU-6, CM-7, CM-8, SC-7.

CM-11 USER-INSTALLED SOFTWARE

[Priority 2]

Control:

- a. Establish agency-level policies governing the installation of software by users;
- b. Enforce software installation policies through automated methods; and
- c. Monitor policy compliance through automated methods at least weekly.

Discussion: If provided the necessary privileges, users can install software in organizational systems. To maintain control over the software installed, organizations identify permitted and prohibited actions regarding software installation. Permitted software installations include updates and security patches to existing software and downloading new applications from organization-approved “app stores.” Prohibited software installations include software with unknown or suspect pedigrees or software that organizations consider potentially malicious. Policies selected for governing user-installed software are organization-developed or provided by some external entity. Policy enforcement methods can include procedural methods and automated methods.

Related Controls: AC-3, AU-6, CM-2, CM-3, CM-5, CM-6, CM-7, CM-8, PL-4, SI-4, SI-7.

CM-12 INFORMATION LOCATION

[Priority 2]

Control:

- a. Identify and document the location of CJI and the specific system components on which the information is processed, stored, or transmitted;
- b. Identify and document the users who have access to the system and system components where the information is processed and stored; and
- c. Document changes to the location (i.e., system or system components) where the information is processed and stored.

Discussion: Information location addresses the need to understand where information is being processed and stored. Information location includes identifying where specific information types and information reside in system components and how information is being processed so that information flow can be understood, and adequate protection and policy management provided for such information and system components. The security category of the information is also a factor in determining the controls necessary to protect the information and the system component where the information resides. The location of the information and system components is also a factor in the architecture and design of the system (see SA-4, SA-8).

Related Controls: AC-2, AC-3, AC-4, AC-6, CM-8, RA-2, SA-4, SA-8, SC-4, SC-28, SI-4, SI-7.

Control Enhancements:

(1) INFORMATION LOCATION | AUTOMATED TOOLS TO SUPPORT INFORMATION LOCATION

[Priority 2]

Control:

Use automated tools to identify CJI on software and hardware system components to ensure controls are in place to protect organizational information and individual privacy.

Discussion: The use of automated tools helps to increase the effectiveness and efficiency of the information location capability implemented within the system. Automation also helps organizations manage the data produced during information location activities and share such information across the organization. The output of automated information location tools can be used to guide and inform system architecture and design decisions.

Related Controls: None.

Figure 5 – A Local Police Department’s Configuration Management Controls

A local police department decided to update their CAD system, and in doing so tracked all changes made to their infrastructure in a configuration management journal, updated their network topology documents to include all new components in their architecture, then marked all documentation as FOUO and stored them securely.

CONTINGENCY PLANNING (CP)

CP-1 POLICY AND PROCEDURES

[Priority 2]

Control:

- a. Develop, document, and disseminate to organizational personnel with contingency planning responsibilities:
 1. Agency-level contingency planning policy that:
 - (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 - (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
 2. Procedures to facilitate the implementation of the contingency planning policy and the associated contingency planning controls;
- b. Designate organizational personnel with information security responsibilities to manage the development, documentation, and dissemination of the contingency planning policy and procedures; and
- c. Review and update the current contingency planning:
 1. Policy annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI, or training simulations or exercises; and
 2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI, or training simulations or exercises.

Discussion: Contingency planning policy and procedures address the controls in the CP family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of contingency planning policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to contingency planning policy and procedures include assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies,

standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PS-8, SI-12.

CP-2 CONTINGENCY PLAN

[Priority 2]

Control:

- a. Develop a contingency plan for the system that:
 1. Identifies essential mission and business functions and associated contingency requirements;
 2. Provides recovery objectives, restoration priorities, and metrics;
 3. Addresses contingency roles, responsibilities, assigned individuals with contact information;
 4. Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure;
 5. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented;
 6. Addresses the sharing of contingency information; and
 7. Is reviewed and approved by agency head or their designee;
- b. Distribute copies of the contingency plan to organizational personnel with contingency planning or incident response duties;
- c. Coordinate contingency planning activities with incident handling activities;
- d. Review the contingency plan for the system annually;
- e. Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;
- f. Communicate contingency plan changes to organizational personnel with contingency planning or incident response duties;
- g. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; and
- h. Protect the contingency plan from unauthorized disclosure and modification.

Discussion: Contingency planning for systems is part of an overall program for achieving continuity of operations for organizational mission and business functions. Contingency planning addresses system restoration and implementation of alternative mission or business processes when systems are compromised or breached. Contingency planning is considered throughout the system development life cycle and is a fundamental part of the system design. Systems can be designed for redundancy, to provide backup capabilities, and for resilience.

Contingency plans reflect the degree of restoration required for organizational systems since not all systems need to fully recover to achieve the level of continuity of operations desired. System recovery objectives reflect applicable laws, executive orders, directives, regulations, policies, standards, guidelines, organizational risk tolerance, and system impact level.

Actions addressed in contingency plans include orderly system degradation, system shutdown, fallback to a manual mode, alternate information flows, and operating in modes reserved for when systems are under attack. By coordinating contingency planning with incident handling activities, organizations ensure that the necessary planning activities are in place and activated in the event of an incident. Incident response planning is part of contingency planning for organizations and is addressed in the IR (Incident Response) family.

Related Controls: CP-3, CP-4, CP-6, CP-7, CP-8, CP-9, CP-10, IR-4, IR-6, IR-8, MA-6, MP-2, MP-4, MP-5, PL-2, SA-15, SC-7, SC-23, SI-12.

Control Enhancements:

(1) CONTINGENCY PLAN | COORDINATE WITH RELATED PLANS

[Priority 2]

Control:

Coordinate contingency plan development with organizational elements responsible for related plans.

Discussion: Plans that are related to contingency plans include Business Continuity Plans, Disaster Recovery Plans, Critical Infrastructure Plans, Continuity of Operations Plans, Crisis Communications Plans, Insider Threat Implementation Plans, Data Breach Response Plans, Cyber Incident Response Plans, Breach Response Plans, and Occupant Emergency Plans.

Related Controls: None.

(3) CONTINGENCY PLAN | RESUME MISSION AND BUSINESS FUNCTIONS

[Priority 2]

Control:

Plan for the resumption of essential mission and business functions within twenty-four (24) hours of contingency plan activation.

Discussion: Organizations may choose to conduct contingency planning activities to resume mission and business functions as part of business continuity planning or as part of business impact analyses. Organizations prioritize the resumption of mission and business functions. The time period for resuming mission and business functions may be dependent on the severity and extent of the disruptions to the system and its supporting infrastructure.

Related Controls: None.

(8) CONTINGENCY PLAN | IDENTIFY CRITICAL ASSETS

[Priority 2]

Control:

Identify critical system assets supporting essential mission and business functions.

Discussion: Organizations may choose to identify critical assets as part of criticality analysis, business continuity planning, or business impact analyses. Organizations identify critical system assets so that additional controls can be employed (beyond the controls routinely implemented) to help ensure that organizational mission and business functions can continue to be conducted during contingency operations. The identification of critical information assets also facilitates the prioritization of organizational resources. Critical system assets include technical and operational aspects. Technical aspects include system components, information technology services, information technology products, and mechanisms. Operational aspects include procedures (i.e., manually executed operations) and personnel (i.e., individuals operating technical controls and/or executing manual procedures). Organizational program protection plans can assist in identifying critical assets.

Related Controls: CM-8, RA-9.

CP-3 CONTINGENCY TRAINING

[Priority 3]

Control:

- a. Provide contingency training to system users consistent with assigned roles and responsibilities:
 1. Within thirty (30) days of assuming a contingency role or responsibility;
 2. When required by system changes; and
 3. Annually thereafter; and
- b. Review and update contingency training content annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI, or training simulations or exercises.

Discussion: Contingency training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail is included in such training. For example, some individuals may only need to know when and where to report for duty during contingency operations and if normal duties are affected; system administrators may require additional training on how to establish systems at alternate processing and storage sites; and organizational officials may receive more specific training on how to conduct mission-essential functions in designated off-site locations and how to establish communications with other governmental entities for purposes of coordination on contingency-related activities. Training for contingency roles or responsibilities reflects the specific continuity requirements in the contingency plan. Events that may precipitate an update to contingency training content include, but are not limited to, contingency plan testing or an actual contingency (lessons learned), assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. At the discretion of the organization, participation in a contingency plan test or exercise, including

lessons learned sessions subsequent to the test or exercise, may satisfy contingency plan training requirements.

Related Controls: AT-2, AT-3, AT-4, CP-2, CP-4, CP-8, IR-2, IR-4.

CP-4 CONTINGENCY PLAN TESTING

[Priority 3]

Control:

- a. Test the contingency plan for the system annually using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: checklists, walk-through and tabletop exercises, simulations (parallel or full interrupt), or comprehensive exercises.
- b. Review the contingency plan test results; and
- c. Initiate corrective actions, if needed.

Discussion: Methods for testing contingency plans to determine the effectiveness of the plans and identify potential weaknesses include checklists, walk-through and tabletop exercises, simulations (parallel or full interrupt), and comprehensive exercises. Organizations conduct testing based on the requirements in contingency plans and include a determination of the effects on organizational operations, assets, and individuals due to contingency operations. Organizations have flexibility and discretion in the breadth, depth, and timelines of corrective actions.

Related Controls: AT-3, CP-2, CP-3, CP-8, CP-9, IR-3, IR-4, PL-2, SR-2.

Control Enhancements:

(1) CONTINGENCY PLAN TESTING | COORDINATE WITH RELATED PLANS

[Priority 3]

Control:

Coordinate contingency plan testing with organizational elements responsible for related plans.

Discussion: Plans related to contingency planning for organizational systems include Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, and Occupant Emergency Plans. Coordination of contingency plan testing does not require organizations to create organizational elements to handle related plans or to align such elements with specific plans. However, it does require that if such organizational elements are responsible for related plans, organizations coordinate with those elements.

Related Controls: IR-8.

CP-6 ALTERNATE STORAGE SITE

[Priority 2]

Control:

- a. Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information; and
- b. Ensure that the alternate storage site provides controls equivalent to that of the primary site.

Discussion: Alternate storage sites are geographically distinct from primary storage sites and maintain duplicate copies of information and data if the primary storage site is not available. Similarly, alternate processing sites provide processing capability if the primary processing site is not available. Geographically distributed architectures that support contingency requirements may be considered alternate storage sites. Items covered by alternate storage site agreements include environmental conditions at the alternate sites, access rules for systems and facilities, physical and environmental protection requirements, and coordination of delivery and retrieval of backup media. Alternate storage sites reflect the requirements in contingency plans so that organizations can maintain essential mission and business functions despite compromise, failure, or disruption in organizational systems.

Related Controls: CP-2, CP-7, CP-8, CP-9, CP-10, MP-4, MP-5, PE-3.

Control Enhancements:

(1) ALTERNATE STORAGE SITE | SEPARATION FROM PRIMARY SITE

[Priority 2]

Control:

Identify an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats.

Discussion: Threats that affect alternate storage sites are defined in organizational risk assessments and include natural disasters, structural failures, hostile attacks, and errors of omission or commission. Organizations determine what is considered a sufficient degree of separation between primary and alternate storage sites based on the types of threats that are of concern. For threats such as hostile attacks, the degree of separation between sites is less relevant.

Related Controls: RA-3.

(3) ALTERNATE STORAGE SITE | ACCESSIBILITY

[Priority 2]

Control:

Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.

Discussion: Area-wide disruptions refer to those types of disruptions that are broad in geographic scope with such determinations made by organizations based on organizational

assessments of risk. Explicit mitigation actions include duplicating backup information at other alternate storage sites if access problems occur at originally designated alternate sites or planning for physical access to retrieve backup information if electronic accessibility to the alternate site is disrupted.

Related Controls: RA-3.

CP-7 ALTERNATE PROCESSING SITE

[Priority 2]

Control:

- a. Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of operations for essential mission and business functions within the time period defined in the system contingency plan(s) when the primary processing capabilities are unavailable;
- b. Make available at the alternate processing site, the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery to the site within the organization-defined time period for transfer and resumption; and
- c. Provide controls at the alternate processing site that are equivalent to those at the primary site.

Discussion: Alternate processing sites are geographically distinct from primary processing sites and provide processing capability if the primary processing site is not available. The alternate processing capability may be addressed using a physical processing site or other alternatives, such as failover to a cloud-based service provider or other internally or externally provided processing service. Geographically distributed architectures that support contingency requirements may also be considered alternate processing sites. Controls that are covered by alternate processing site agreements include the environmental conditions at alternate sites, access rules, physical and environmental protection requirements, and the coordination for the transfer and assignment of personnel. Requirements are allocated to alternate processing sites that reflect the requirements in contingency plans to maintain essential mission and business functions despite disruption, compromise, or failure in organizational systems.

Related Controls: CP-2, CP-6, CP-8, CP-9, CP-10, MA-6, PE-3, PE-11, PE-12, PE-17.

Control Enhancements:

(1) ALTERNATE PROCESSING SITE | SEPARATION FROM PRIMARY SITE

[Priority 2]

Control:

Identify an alternate processing site that is sufficiently separated from the primary processing site to reduce susceptibility to the same threats.

Discussion: Threats that affect alternate processing sites are defined in organizational assessments of risk and include natural disasters, structural failures, hostile attacks, and errors of omission or commission. Organizations determine what is considered a sufficient degree of separation between primary and alternate processing sites based on the types of threats that are of concern. For threats such as hostile attacks, the degree of separation between sites is less relevant.

Related Controls: RA-3.

(2) ALTERNATE PROCESSING SITE | ACCESSIBILITY

[Priority 2]

Control:

Identify potential accessibility problems to alternate processing sites in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

Discussion: Area-wide disruptions refer to those types of disruptions that are broad in geographic scope with such determinations made by organizations based on organizational assessments of risk.

Related Controls: RA-3.

(3) ALTERNATE PROCESSING SITE | PRIORITY OF SERVICE

[Priority 2]

Control:

Develop alternate processing site agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives).

Discussion: Priority of service agreements refer to negotiated agreements with service providers that ensure that organizations receive priority treatment consistent with their availability requirements and the availability of information resources for logical alternate processing and/or at the physical alternate processing site. Organizations establish recovery time objectives as part of contingency planning.

Related Controls: None.

CP-8 TELECOMMUNICATIONS SERVICES

[Priority 2]

Control:

Establish alternate telecommunications services, including necessary agreements to permit the resumption of system operations for essential mission and business functions within the time period as defined in the system contingency plan(s) when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

Discussion: Telecommunications services (for data and voice) for primary and alternate processing and storage sites are in scope for CP-8. Alternate telecommunications services reflect

the continuity requirements in contingency plans to maintain essential mission and business functions despite the loss of primary telecommunications services. Organizations may specify different time periods for primary or alternate sites. Alternate telecommunications services include additional organizational or commercial ground-based circuits or lines, network-based approaches to telecommunications, or the use of satellites. Organizations consider factors such as availability, quality of service, and access when entering into alternate telecommunications agreements.

Related Controls: CP-2, CP-6, CP-7, SC-7.

Control Enhancements:

(1) TELECOMMUNICATIONS SERVICES | PRIORITY OF SERVICE PROVISIONS

[Priority 2]

Control:

- a. Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives); and
- b. Request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness if the primary and/or alternate telecommunications services are provided by a common carrier.

Discussion: Organizations consider the potential mission or business impact in situations where telecommunications service providers are servicing other organizations with similar priority of service provisions. Telecommunications Service Priority (TSP) is a Federal Communications Commission (FCC) program that directs telecommunications service providers (e.g., wireline and wireless phone companies) to give preferential treatment to users enrolled in the program when they need to add new lines or have their lines restored following a disruption of service, regardless of the cause. The FCC sets the rules and policies for the TSP program, and the Department of Homeland Security manages the TSP program. The TSP program is always in effect and not contingent on a major disaster or attack taking place. Federal sponsorship is required to enroll in the TSP program.

Related Controls: None.

(2) TELECOMMUNICATIONS SERVICES | SINGLE POINTS OF FAILURE

[Priority 2]

Control:

Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

Discussion: In certain circumstances, telecommunications service providers or services may share the same physical lines, which increases the vulnerability of a single failure point. It is

important to have provider transparency for the actual physical transmission capability for telecommunication services.

Related Controls: None.

CP-9 SYSTEM BACKUP

[Priority 2]

Control:

- a. Conduct backups of user-level information contained in operational systems for essential business functions as required by the contingency plans;
- b. Conduct backups of system-level information contained in the system as required by the contingency plans;
- c. Conduct backups of system documentation, including security- and privacy-related documentation as required by the contingency plans; and
- d. Protect the confidentiality, integrity, and availability of backup information.

Discussion: System-level information includes system state information, operating system software, middleware, application software, and licenses. User-level information includes information other than system-level information. Mechanisms employed to protect the integrity of system backups include digital signatures and cryptographic hashes. Protection of system backup information while in transit is addressed by MP-5 and SC-8. System backups reflect the requirements in contingency plans as well as other organizational requirements for backing up information. Organizations may be subject to laws, executive orders, directives, regulations, or policies with requirements regarding specific categories of information (e.g., criminal justice information). Organizational personnel consult with the senior agency official for privacy and legal counsel regarding such requirements.

Related Controls: CP-2, CP-6, CP-10, MP-4, MP-5, SC-8, SC-12, SC-13, SI-4.

Control Enhancements:

(1) SYSTEM BACKUP | TESTING FOR RELIABILITY AND INTEGRITY

[Priority 2]

Control:

Test backup information as required by the contingency plans to verify media reliability and information integrity.

Discussion: Organizations need assurance that backup information can be reliably retrieved. Reliability pertains to the systems and system components where the backup information is stored, the operations used to retrieve the information, and the integrity of the information being retrieved. Independent and specialized tests can be used for each of the aspects of reliability. For example, decrypting and transporting (or transmitting) a random sample of backup files from the alternate storage or backup site and comparing the information to the same information at the primary processing site can provide such assurance.

Related Controls: CP-4.

(8) SYSTEM BACKUP | CRYPTOGRAPHIC PROTECTION

[Priority 2]

Control:

Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of CJI.

Discussion: The selection of cryptographic mechanisms is based on the need to protect the confidentiality and integrity of backup information. The strength of mechanisms selected is commensurate with the security category or classification of the information. Cryptographic protection applies to system backup information in storage at both primary and alternate locations. Organizations that implement cryptographic mechanisms to protect information at rest also consider cryptographic key management solutions.

Related Controls: SC-12, SC-13, SC-28.

CP-10 SYSTEM RECOVERY AND RECONSTITUTION

[Priority 2]

Control:

Provide for the recovery and reconstitution of the system to a known state within the timeframe as required by the contingency plans after a disruption, compromise, or failure.

Discussion: Recovery is executing contingency plan activities to restore organizational mission and business functions. Reconstitution takes place following recovery and includes activities for returning systems to fully operational states. Recovery and reconstitution operations reflect mission and business priorities; recovery point, recovery time, and reconstitution objectives; and organizational metrics consistent with contingency plan requirements. Reconstitution includes the deactivation of interim system capabilities that may have been needed during recovery operations. Reconstitution also includes assessments of fully restored system capabilities, reestablishment of continuous monitoring activities, system reauthorization (if required), and activities to prepare the system and organization for future disruptions, breaches, compromises, or failures. Recovery and reconstitution capabilities can include automated mechanisms and manual procedures. Organizations establish recovery time and recovery point objectives as part of contingency planning.

Related Controls: CP-2, CP-4, CP-6, CP-7, CP-9, IR-4, SA-8.

Control Enhancements:

(2) SYSTEM RECOVERY AND RECONSTITUTION | TRANSACTION RECOVERY

[Priority 2]

Control:

Implement transaction recovery for systems that are transaction-based.

Discussion: Transaction-based systems include database management systems and transaction processing systems. Mechanisms supporting transaction recovery include transaction rollback and transaction journaling.

Related Controls: None.

IDENTIFICATION AND AUTHENTICATION (IA)

Identification is a unique, auditable representation of an identity within an information system usually in the form of a simple character string for each individual user, machine, software component, or any other entity. Authentication refers to mechanisms or processes to verify the identity of a user, process, or device, as a prerequisite to allowing access to a system's resources.

IA-0 USE OF ORIGINATING AGENCY IDENTIFIERS IN TRANSACTIONS AND INFORMATION EXCHANGES

[Existing]

An FBI authorized originating agency identifier (ORI) shall be used in each transaction on CJIS systems in order to identify the sending agency and to ensure the proper level of access for each transaction. The original identifier between the requesting agency and the CSA/SIB/Channeler shall be the ORI, and other agency identifiers, such as user identification or personal identifier, an access device mnemonic, or the Internet Protocol (IP) address.

Agencies may act as a servicing agency and perform transactions on behalf of authorized agencies requesting the service. Servicing agencies performing inquiry transactions on behalf of another agency may do so using the requesting agency's ORI. Servicing agencies may also use their own ORI to perform inquiry transactions on behalf of a requesting agency if the means and procedures are in place to provide an audit trail for the current specified retention period. Because the agency performing the transaction may not necessarily be the same as the agency requesting the transaction, the CSA/SIB/Channeler shall ensure that the ORI for each transaction can be traced, via audit trail, to the specific agency which is requesting the transaction.

Audit trails can be used to identify the requesting agency if there is a reason to inquire into the details surrounding why an agency ran an inquiry on a subject. Agencies assigned a limited access ORI shall not use the full access ORI of another agency to conduct an inquiry transaction.

NOTE: This control will be included in AC-3 Access Enforcement when modernized.

IA-1 POLICY AND PROCEDURES

[Priority 2]

Control:

- a. Develop, document, and disseminate to authorized personnel:
 1. Agency/Entity identification and authentication policy that:
 - (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 - (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
 2. Procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls;
- b. Designate an individual with security responsibilities to manage the development, documentation, and dissemination of the identification and authentication policy and procedures; and

- c. Review and update the current identification and authentication:
 - 1. Policy annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI; and
 - 2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.

DISCUSSION: Identification and authentication policy and procedures address the controls in the IA family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of identification and authentication policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to identification and authentication policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: AC-1, PS-8, SI-12.

Control Enhancements: None.

IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

[Existing] [Priority 1]

Control:

Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

DISCUSSION: Organizations can satisfy the identification and authentication requirements by complying with the requirements in [HSPD 12]. Organizational users include employees or individuals who organizations consider to have an equivalent status to employees (e.g., contractors and guest researchers). Unique identification and authentication of users applies to all accesses other than those that are explicitly identified in AC-14 and that occur through the authorized use of group authenticators without individual authentication. Since processes execute on behalf of groups and roles, organizations may require unique identification of individuals in group accounts or for detailed accountability of individual activity.

Organizations employ passwords, physical authenticators, or biometrics to authenticate user identities or, in the case of multi-factor authentication, some combination thereof. Access to organizational systems is defined as either local access or network access. Local access is any access to organizational systems by users or processes acting on behalf of users, where access is

obtained through direct connections without the use of networks. Network access is access to organizational systems by users (or processes acting on behalf of users) where access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks. Internal networks include local area networks and wide area networks.

The use of encrypted virtual private networks for network connections between organization-controlled endpoints and non-organization-controlled endpoints may be treated as internal networks with respect to protecting the confidentiality and integrity of information traversing the network. Identification and authentication requirements for non-organizational users are described in IA-8.

Related Controls: AC-2, AC-3, AC-4, AC-14, AC-17, AC-18, AU-1, AU-6, IA-4, IA-5, IA-8, MA-4, MA-5, PE-2, PL-4, SA-4, SA-8.

Control Enhancements:

(1) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | MULTI-FACTOR AUTHENTICATION TO PRIVILEGED ACCOUNTS

[Priority 1]

Control:

Implement multi-factor authentication for access to privileged accounts.

DISCUSSION: Multi-factor authentication requires the use of two or more different factors to achieve authentication. The authentication factors are defined as follows: something you know (e.g., a personal identification number [PIN]), something you have (e.g., a physical authenticator such as a cryptographic private key), or something you are (e.g., a biometric). Multi-factor authentication solutions that feature physical authenticators include hardware authenticators that provide time-based or challenge-response outputs and smart cards such as the U.S. Government Personal Identity Verification (PIV) card or the Department of Defense (DoD) Common Access Card (CAC). In addition to authenticating users at the system level (i.e., at logon), organizations may employ authentication mechanisms at the application level, at their discretion, to provide increased security. Regardless of the type of access (i.e., local, network, remote), privileged accounts are authenticated using multi-factor options appropriate for the level of risk. Organizations can add additional security measures, such as additional or more rigorous authentication mechanisms, for specific types of access.

Related Controls: AC-5, AC-6.

(2) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | MULTI-FACTOR AUTHENTICATION TO NON-PRIVILEGED ACCOUNTS

[Priority 1]

Control:

Implement multi-factor authentication for access to non-privileged accounts.

DISCUSSION: Multi-factor authentication requires the use of two or more different factors to achieve authentication. The authentication factors are defined as follows: something you know

(e.g., a personal identification number [PIN]), something you have (e.g., a physical authenticator such as a cryptographic private key), or something you are (e.g., a biometric). Multi-factor authentication solutions that feature physical authenticators include hardware authenticators that provide time-based or challenge-response outputs and smart cards such as the U.S. Government Personal Identity Verification card or the DoD Common Access Card. In addition to authenticating users at the system level, organizations may also employ authentication mechanisms at the application level, at their discretion, to provide increased information security. Regardless of the type of access (i.e., local, network, remote), non-privileged accounts are authenticated using multi-factor options appropriate for the level of risk. Organizations can provide additional security measures, such as additional or more rigorous authentication mechanisms, for specific types of access.

Related Controls: AC-5.

(8) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | ACCESS TO ACCOUNTS — REPLAY RESISTANT

[Priority 1]

Control:

Implement replay-resistant authentication mechanisms for access to privileged and non-privileged accounts.

DISCUSSION: Authentication processes resist replay attacks if it is impractical to achieve successful authentications by replaying previous authentication messages. Replay-resistant techniques include protocols that use nonces or challenges such as time synchronous or cryptographic authenticators.

Related Controls: None.

(12) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | ACCEPTANCE OF PIV CREDENTIALS

[Priority 1]

Control:

Accept and electronically verify Personal Identity Verification-compliant credentials.

DISCUSSION: Acceptance of Personal Identity Verification (PIV)-compliant credentials applies to organizations implementing logical access control and physical access control systems. PIV-compliant credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. The adequacy and reliability of PIV card issuers are authorized using [SP 800-79-2]. Acceptance of PIV-compliant credentials includes derived PIV credentials, the use of which is addressed in [SP 800-166]. The DOD Common Access Card (CAC) is an example of a PIV credential.

Related Controls: None.

IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION

[Priority 2]

Control:

Uniquely identify and authenticate agency-managed devices before establishing network connections. In the instance of local connection, the device must be approved by the agency and the device must be identified and authenticated prior to connection to an agency asset.

DISCUSSION: Devices that require unique device-to-device identification and authentication are defined by type, device, or a combination of type and device. Organization-defined device types include devices that are not owned by the organization. Systems use shared known information (e.g., Media Access Control [MAC], Transmission Control Protocol/Internet Protocol [TCP/IP] addresses) for device identification or organizational authentication solutions (e.g., Institute of Electrical and Electronics Engineers (IEEE) 802.1x and Extensible Authentication Protocol [EAP], RADIUS server with EAP-Transport Layer Security [TLS] authentication, Kerberos) to identify and authenticate devices on local and wide area networks. Organizations determine the required strength of authentication mechanisms based on the security categories of systems and mission or business requirements. Because of the challenges of implementing device authentication on a large scale, organizations can restrict the application of the control to a limited number/type of devices based on mission or business needs.

Related Controls: AC-17, AC-18, AC-19, AU-6, CA-3, CA-9, IA-4, IA-5, IA-11, SI-4.

IA-4 IDENTIFIER MANAGEMENT

[Existing] [Priority 2]

Control:

Manage system identifiers by:

- a. Receiving authorization from organizational personnel with identifier management responsibilities to assign an individual, group, role, service, or device identifier;
- b. Selecting an identifier that identifies an individual, group, role, service, or device;
- c. Assigning the identifier to the intended individual, group, role, service, or device; and
- d. Preventing reuse of identifiers for one (1) year.

DISCUSSION: Common device identifiers include Media Access Control (MAC) addresses, Internet Protocol (IP) addresses, or device-unique token identifiers. The management of individual identifiers is not applicable to shared system accounts. Typically, individual identifiers are the usernames of the system accounts assigned to those individuals. In such instances, the account management activities of AC-2 use account names provided by IA-4. Identifier management also addresses individual identifiers not necessarily associated with system accounts. Preventing the reuse of identifiers implies preventing the assignment of previously used individual, group, role, service, or device identifiers to different individuals, groups, roles, services, or devices.

Related Controls: AC-5, IA-2, IA-3, IA-5, IA-8, IA-12, MA-4, PE-2, PE-3, PE-4, PL-4, PS-3, PS-4, PS-5.

Control Enhancements:

(4) IDENTIFIER MANAGEMENT | IDENTIFY USER STATUS

[Priority 2]

Control:

Manage individual identifiers by uniquely identifying each individual as agency or nonagency.

DISCUSSION: Characteristics that identify the status of individuals include contractors, foreign nationals, and non-organizational users. Identifying the status of individuals by these characteristics provides additional information about the people with whom organizational personnel are communicating. For example, it might be useful for a government employee to know that one of the individuals on an email message is a contractor.

Related Controls: None.

IA-5 AUTHENTICATOR MANAGEMENT

[Priority 1]

Control:

Manage system authenticators by:

- a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator;
- b. Establishing initial authenticator content for any authenticators issued by the organization;
- c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
- d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators;
- e. Changing default authenticators prior to first use;
- f. Changing or refreshing memorized secret authenticators annually or when there is evidence of authenticator compromise; changing or refreshing all other authenticator types as they expire or when there is evidence of authenticator compromise;
- g. Protecting authenticator content from unauthorized disclosure and modification;
- h. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and
- i. Changing authenticators for group or role accounts when membership to those accounts changes.
- j. AAL2 Specific Requirements

Control:

All credential service providers (CSPs) authenticating claimants at Authenticator Assurance Level 2 (AAL2) SHALL be assessed on the following criteria:

- (1) Authentication SHALL occur by the use of either a multi-factor authenticator or a combination of two single-factor authenticators.

SUPPLEMENTAL GUIDANCE: A multi-factor authenticator requires two factors to execute a single authentication event, such as a cryptographically-secure device with an integrated biometric sensor that is required to activate the device. Nine different authenticator types are recognized, representing something you know (a memorized secret), something you have (a physical authenticator), or combinations of physical authenticators with either memorized secrets or biometric modalities (something you are). Multi-factor (MF) authentication is required at AAL2. MF authentication at AAL2 may be performed using the following AAL2 permitted authenticator types: MF OTP Device, MF Crypto Software, or MF Crypto Device; or a memorized secret used in combination with the following permitted single-factor authenticators: Look-Up Secret, Out-of-Band authenticator, SF OTP Device, SF Crypto Software, or SF Crypto Device.

- (2) If the multi-factor authentication process uses a combination of two single-factor authenticators, then it SHALL include a Memorized Secret authenticator and a possession-based authenticator.

SUPPLEMENTAL GUIDANCE: Multifactor authentication requires the use of two different authentication factors. See IA-5 j (1) for permitted authenticator types at AAL2.

- (3) Cryptographic authenticators used at AAL2 SHALL use approved cryptography.

SUPPLEMENTAL GUIDANCE: Cryptography is considered approved if it is specified or adopted in a FIPS or NIST recommendation. Since verifiers and cryptographic authenticators must use the same algorithms to successfully authenticate, assessment of the verifier also assesses the authenticators that may be used.

- (4) At least one authenticator used at AAL2 SHALL be replay resistant.

SUPPLEMENTAL GUIDANCE: Replay resistance is a characteristic of most, although not all, physical authenticators. A given output of the authenticator is required to be accepted for only one authentication transaction. For example, the output of a time-based OTP device or an out-of-band device is considered replay resistant if it can only be used for at most one authentication transaction during its validity period. If it can be used for more than one during this period, it is not replay resistant.

- (5) Communication between the claimant and verifier SHALL be via an authenticated protected channel.

SUPPLEMENTAL GUIDANCE: Communication between claimant or user and verifier or agency is required to be via an encrypted channel that authenticates the verifier to provide confidentiality of the authenticator output and resistance to Man-in-the-Middle (MitM) attacks. This is typically accomplished using the Transport Level Security (TLS) protocol. Mutual authentication of the communication channel is not required unless that is part of the process of authenticating the claimant. Accordingly, the verifier is only responsible the use of an appropriately secure communications protocol.

- (6) Verifiers operated by government agencies at AAL2 SHALL be validated to meet the requirements of FIPS 140 Level 1.

SUPPLEMENTAL GUIDANCE: Verifiers operated by or on behalf of government agencies are required to be validated to meet FIPS 140 requirements. The FIPS 140 requirements generally apply to cryptographic modules (both hardware and software).

- (7) Authenticators procured by government agencies SHALL be validated to meet the requirements of FIPS 140 Level 1.

SUPPLEMENTAL GUIDANCE: The FIPS 140 requirements generally apply to cryptographic modules (both hardware and software). While authenticators are not directly the responsibility of the CSP (particularly in the case of bring- your-own authenticators), the CSP is still responsible for ensuring that a sufficiently strong and FIPS 140 validated authenticator is being used. Binding of CSP-supplied authenticators that are known to meet validation criteria is sufficient.

- (8) If a device such as a smartphone is used in the authentication process, then the unlocking of that device (typically done using a PIN or biometric) SHALL NOT be considered one of the authentication factors.

SUPPLEMENTAL GUIDANCE: This requirement applies to multi-factor authenticators resident on a smartphone or similar device; single-factor authenticators on such devices would only provide a single (physical) authentication factor. Unlocking of a device such as a smartphone may be done for any number of reasons unrelated to authentication, and such devices are normally in an unlocked state for a period of time thereafter. Human action such as entry of a memorized secret or presentation of a biometric factor needs to be provided that is directly associated with the authentication event. Generally, it is not possible for a verifier to know that the device had been locked or if the unlock process met the requirements for the relevant authenticator type.

- (9) If a biometric factor is used in authentication at AAL2, then the performance requirements stated in IA-5 m Biometric Requirements SHALL be met.

SUPPLEMENTAL GUIDANCE: Detailed conformance criteria applicable to the use of biometrics are contained in section IA-5 m Biometric Requirements. Since verification of biometric factors is not deterministic due to measurement errors in collection of the

biometric information, evaluation of performance, and, most importantly, false accept rate, is important to ensure security of the authentication process.

(10) Reauthentication of the subscriber SHALL be repeated at least once per 12 hours during an extended usage session.

SUPPLEMENTAL GUIDANCE: Reauthentication is required to mitigate the risks associated with an authenticated endpoint that has been abandoned by the subscriber or has been misappropriated by an attacker while authenticated. At AAL2, providing a memorized secret or biometric factor is sufficient for reauthentication prior to the expiration time.

(11) Reauthentication of the subscriber SHALL be repeated following any period of inactivity lasting 30 minutes or longer.

SUPPLEMENTAL GUIDANCE: Reauthentication is required to mitigate the risks associated with an authenticated endpoint that has been abandoned by the subscriber or has been misappropriated by an attacker while authenticated. At AAL2, providing a memorized secret or biometric factor is sufficient for reauthentication prior to the expiration time.

(12) The CSP SHALL employ appropriately tailored security controls from the moderate baseline of security controls defined in the CJISSECPOL.

The CSP SHALL ensure that the minimum assurance-related controls for moderate-impact systems are satisfied.

SUPPLEMENTAL GUIDANCE: NIST SP 800-53 provides a comprehensive catalog of controls, three security control baselines (low, moderate, and high impact), and guidance for tailoring the appropriate baseline to specific needs and risk environments for federal information systems. These controls are the operational, technical, and management safeguards to maintain the integrity, confidentiality, and security of federal information systems and are intended to be used in conjunction with the NIST risk management framework outlined in SP 800-37 and SP 800-63-3 section 5 Digital Identity Risk Management. NIST SP 800-53 presents security control baselines determined by the security categorization of the information system (low, moderate or high) from NIST FIPS 199 Standards for Security Categorization of Federal Information and Information Systems. For IAL2, the moderate baseline controls (see <https://nvd.nist.gov/800-53/Rev4/impact/moderate>) may be considered the starting point for the selection, enhancement, and tailoring of the security controls presented. Guidance on tailoring the control baselines to best meet the organization's risk environment, systems and operations is presented in SP 800-53 section 3.2. Tailoring Baseline Security Controls.

While SP 800-53 and other NIST Special Publications in the SP-800-XXX series apply to federal agencies for the implementation of the Federal Information Security Management Act (FISMA), non-federal entities providing services for federal information services also are subject to FISMA and should similarly use SP 800-53 and associated publications for appropriate controls. Non-federal entities may be subject to and conformant with other

applicable controls systems and processes for information system security (e.g., FEDRAMP, ISO/IEC 27001). SP-63A allows the application of equivalent controls from such standards and processes to meet conformance with this criterion.

- (13) The CSP SHALL comply with records retention policies in accordance with applicable laws and regulations.

SUPPLEMENTAL GUIDANCE: It is recommended that CSPs document any specific retention policies they are subject to, in accordance with applicable laws, regulations, or policies, including any National Archives and Records Administration (NARA) records retention schedules that may apply.

The CSP is responsible for the proper handling, protection, and retention or disposal of any sensitive data it collects, even after it ceases to provide identity proofing and enrollment services. A CSP may document its policies and procedures for the management of the data it collects in a data handling plan or other document.

- (14) If the CSP opts to retain records in the absence of any mandatory requirements, then the CSP SHALL conduct a risk management process, including assessments of privacy and security risks to determine how long records should be retained and SHALL inform subscribers of that retention policy.

SUPPLEMENTAL GUIDANCE: This is a conditional requirement and depends on the basis for CSP records retention. Absent clear jurisdictional requirements, risk management processes, including privacy and security risk assessment, need to be performed for records retention decisions. The records retention duration is required to be derived from a risk-based decision process.

k. Privacy requirements that apply to all CSPs, verifiers, and RPs.

- (1) The CSP SHALL employ appropriately tailored privacy controls from the CJISSECPOL.

SUPPLEMENTAL GUIDANCE: This requirement establishes overall privacy posture of the CSP.

- (2) If the CSP processes attributes for purposes other than identity proofing, authentication, or attribute assertions (collectively “identity service”), related fraud mitigation, or to comply with law or legal process, then the CSP SHALL implement measures to maintain predictability and manageability commensurate with the associated privacy risk.

SUPPLEMENTAL GUIDANCE: Predictability and manageability measures include providing clear notice, obtaining subscriber consent, and enabling selective use and disclosure of attributes. Predictability is meant to build trust and provide accountability and

requires full understanding (and disclosure) of how the attribute information will be used. Manageability also builds trust by demonstrating a CSPs ability to control attribute information throughout processing – collection, maintenance, retention.

1. General requirements applicable to AAL2 authentication process.

- (1) CSPs SHALL provide subscriber instructions on how to appropriately protect a physical authenticator against theft or loss.

SUPPLEMENTAL GUIDANCE: Instruction should address aspects of protecting the specific type of authenticator being used.

- (2) The CSP SHALL provide a mechanism to revoke or suspend the authenticator immediately upon notification from subscriber that loss or theft of the authenticator is suspected.

SUPPLEMENTAL GUIDANCE: The CSP needs to have a documented procedure to allow subscribers to report lost or stolen physical authenticators, and to revoke or suspend such authenticators promptly when reported. Subscribers need to be instructed (see GEN-1) the procedure for reporting loss or theft.

- (3) If required by the authenticator type descriptions in IA-5(1), then the verifier SHALL implement controls to protect against online guessing attacks.

SUPPLEMENTAL GUIDANCE: Throttling or rate limiting is key to resistance against online guessing attacks. This is generally required for memorized secrets or when the authenticator output of a look-up secret, OOB, or OTP authenticator may have less than 64 bits of entropy.

- (4) If required by the authenticator type descriptions in IA-5(1) and the description of a given authenticator does not specify otherwise, then the verifier SHALL limit consecutive failed authentication attempts on a single account to no more than 100.

SUPPLEMENTAL GUIDANCE: Throttling or rate limiting is key to resistance against online guessing attacks. It is important that it be implemented in a non-abrupt manner as described in the specification so that it is not usable as a denial-of-service mechanism by an attacker. Additional techniques MAY be used to reduce the likelihood that an attacker will lock the legitimate claimant out as a result of rate limiting. These include:

- Requiring the claimant to complete a CAPTCHA before attempting authentication.
- Requiring the claimant to wait following a failed attempt for a period of time that increases as the account approaches its maximum allowance for consecutive failed attempts (e.g., 30 seconds up to an hour).

- Accepting only authentication requests that come from a white list of IP addresses from which the subscriber has been successfully authenticated before. Leveraging other risk-based or adaptive authentication techniques to identify user behavior that falls within, or out of, typical norms. These might, for example, include use of IP address, geolocation, timing of request patterns, or browser metadata.

(5) If signed attestations are used, then they SHALL be signed using a digital signature that provides at least the minimum security strength specified in the latest revision of 112 bits as of the date of this publication.

SUPPLEMENTAL GUIDANCE: Attestations are sometimes provided by cryptographic authenticators to securely indicate their capabilities, e.g., that they are hardware-based or that they have characteristics such as two-factor capability. For the attestations to be useful, these signatures need to use algorithms and keys that are sufficiently strong.

(6) If the verifier and CSP are separate entities (as shown by the dotted line in Figure 8 Digital Identity Model), then communications between the verifier and CSP SHALL occur through a mutually-authenticated secure channel (such as a client-authenticated TLS connection).

SUPPLEMENTAL GUIDANCE: In cases where the verifier and CSP are separate, it is important that this not create additional security vulnerabilities as compared with an integrated verifier/CSP combination. This requirement ensures that there is not an opportunity to perform eavesdropping or active attacks on the channel between them.

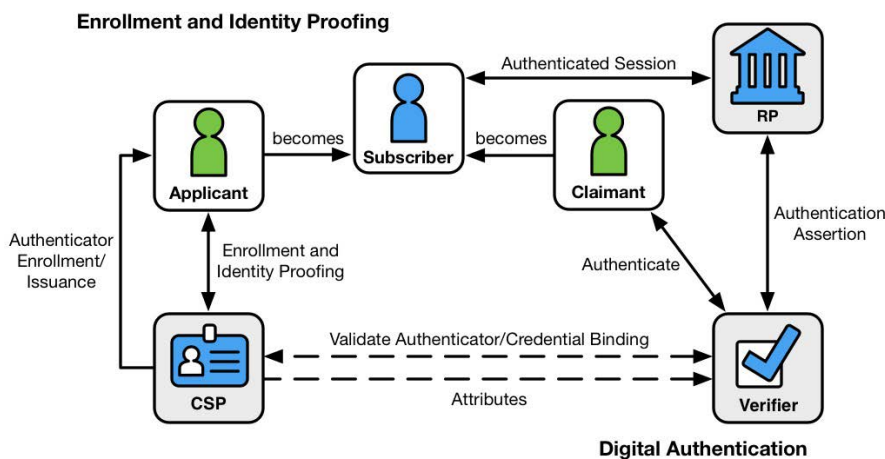


Figure 6 – Digital Identity Model

(7) If the CSP provides the subscriber with a means to report loss, theft, or damage to an authenticator using a backup or alternate authenticator, then that authenticator SHALL be either a memorized secret or a physical authenticator.

SUPPLEMENTAL GUIDANCE: It is important that the loss of control of an authenticator be quickly reported to the CSP. To balance between the need to easily and promptly report this and the risk of a fraudulent report, a backup authenticator, either a memorized

secret or physical authenticator, should be usable by the subscriber to make this report. Only a single, single-factor authenticator is required.

- (8) If the CSP chooses to verify an address of record (i.e., email, telephone, postal) and suspend authenticator(s) reported to have been compromised, then...The suspension SHALL be reversible if the subscriber successfully authenticates to the CSP using a valid (i.e., not suspended) authenticator and requests reactivation of an authenticator suspended in this manner.

SUPPLEMENTAL GUIDANCE: Reversibility of suspension is intended to minimize the impact of inadvertent loss reports from the subscriber and in some cases from an attacker who may be attempting to deny service to the subscriber.

- (9) If and when an authenticator expires, it SHALL NOT be usable for authentication.

SUPPLEMENTAL GUIDANCE: Expiration is used by some CSPs to limit the security exposure from an authenticator that is lost but the loss has not been detected/reported and revoked.

- (10) The CSP SHALL have a documented process to require subscribers to surrender or report the loss of any physical authenticator containing attribute certificates signed by the CSP as soon as practical after expiration or receipt of a renewed authenticator.

SUPPLEMENTAL GUIDANCE: The requirement for surrender or destruction of expired authenticators minimizes the possibility that authentication with an expired authenticator will be attempted. PKI-based authenticators that are collected or known to be destroyed also do not need to be included in certificate revocation lists.

- (11) CSPs SHALL revoke the binding of authenticators immediately upon notification when an online identity ceases to exist (e.g., subscriber's death, discovery of a fraudulent subscriber), when requested by the subscriber, or when the CSP determines that the subscriber no longer meets its eligibility requirements.

SUPPLEMENTAL GUIDANCE: Prompt revocation ensures that unauthorized parties are not able to use the authenticator to make unauthorized access to the subscriber account. Revocation at subscriber request can affect only a single authenticator; the other classes of revocation generally affect all authenticators associated with the subscriber's account.

- (12) The CSP SHALL have a documented process to require subscribers to surrender or report the loss of any physical authenticator containing certified attributes signed by the CSP within five (5) days after revocation or termination takes place.

SUPPLEMENTAL GUIDANCE: This requirement blocks the use of the authenticator's certified attributes in offline situations between revocation/termination and expiration

of the certification. Prompt revocation ensures that unauthorized parties are not able to use the authenticator to make unauthorized access to the subscriber account. Collection or destruction also minimizes the dependence on (and growth of) certificate revocation lists, which are not always 100% effective in accomplishing revocation, particularly in offline situations.

m. Biometric Requirements

- (1) Biometrics SHALL be used only as part of multi-factor authentication with a physical authenticator (something you have).

SUPPLEMENTAL GUIDANCE: For a variety of reasons listed here, a biometric factor is not considered to be an authenticator by itself. The risks associated with biometric factors are largely mitigated by binding the biometric with a specific physical authenticator.

- The biometric False Match Rate (FMR) does not provide confidence in the authentication of the subscriber by itself. In addition, FMR does not account for spoofing attacks.
- Biometric comparison is probabilistic, whereas the other authentication factors are deterministic.
- Biometric template protection schemes provide a method for revoking biometric credentials that is comparable to other authentication factors (e.g., PKI certificates and passwords). However, the availability of such solutions is limited, and standards for testing these methods are under development.
- Biometric characteristics do not constitute secrets. They can be obtained online or by taking a picture of someone with a camera phone (e.g., facial images) with or without their knowledge, lifted from objects someone touches (e.g., latent fingerprints), or captured with high resolution images (e.g., iris patterns). While presentation attack detection (PAD) technologies (e.g., liveness detection) can mitigate the risk of these types of attacks, additional trust in the sensor or biometric processing is required to ensure that PAD is operating in accordance with the needs of the CSP and the subscriber.

- (2) An authenticated protected channel between sensor (or an endpoint containing a sensor that resists sensor replacement) and verifier SHALL be established.

SUPPLEMENTAL GUIDANCE: This requirement ensures that biometric data that flows across the network to the verifier is protected from disclosure and that an attacker cannot substitute a “skimmer” or other fraudulent replacement for the biometric sensor. If the biometric factor is verified directly on a multi-factor authenticator and the sensor

is tightly integrated with it, that local connection does not require an authenticated protected channel.

- (3) The sensor or endpoint SHALL be authenticated prior to capturing the biometric sample from the claimant.

SUPPLEMENTAL GUIDANCE: This requirement ensures that the biometric data being verified is obtained from the expected sensor rather than from a device that may be spoofing biometric information. This is generally not required when the biometric factor is verified in an endpoint that is tightly integrated with the sensor in a manner that resists sensor replacement.

- (4) The biometric system SHALL operate with an FMR [ISO/IEC 2382-37] of 1 in 1000 or better. This FMR SHALL be achieved under conditions of a conformant attack (i.e., zero-effort impostor attempt) as defined in [ISO/IEC 30107-1].

SUPPLEMENTAL GUIDANCE: Since biometric comparison is an approximate match, an operating point threshold is chosen by the verifier that balances false matches and false non-matches. To operate adequately as a verifier, a 1 in 1000 or better false match rate is required.

- (5) The biometric system SHALL allow no more than 5 consecutive failed authentication attempts or 10 consecutive failed attempts if PAD demonstrating at least 90% resistance to presentation attacks is implemented.

SUPPLEMENTAL GUIDANCE: With a false accept rate of as much as 1 in 1000 zero-effort attempts, the ability to make a large number of biometric authentication attempts would result in an unacceptably high probability of mis-authentication. This limit is comparable to that provided by several commercial products (mobile devices) currently on the market.

- (6) Once the limit on authentication failures has been reached, the biometric authenticator SHALL either:
- i. Impose a delay of at least 30 seconds before the next attempt, increasing exponentially with each successive attempt, or
 - ii. disable the biometric user authentication and offer another factor (e.g., a different biometric modality or a PIN/Passcode if it is not already a required factor) if such an alternative method is already available.

SUPPLEMENTAL GUIDANCE: Following a number of consecutive biometric match failures that exceeds the limit in IA-5 m (5), subsequent attempts need to be either aggressively delayed (e.g., 1 minute before the following failed attempt, 2 minutes before the second following attempt) or another authentication or biometric modality associated with the same physical authenticator needs to be used.

- (7) The verifier SHALL make a determination of sensor and endpoint performance, integrity, and authenticity.

SUPPLEMENTAL GUIDANCE: The verifier needs to have a basis for determining that biometric verification meets the necessary performance requirements. This may be accomplished by authenticating the sensor or endpoint, by a certification by an approved accreditation authority, or by runtime interrogation of a signed attestation.

- (8) If biometric comparison is performed centrally, then use of the biometric as an authentication factor SHALL be limited to one or more specific devices that are identified using approved cryptography.

SUPPLEMENTAL GUIDANCE: The ability to use a biometric factor on an arbitrary device greatly increases the value of breached biometric data. For this reason, the use of the biometric factor is limited to specific devices for each subscriber. A separate key is required since the main authentication key is only unlocked upon successful comparison of the biometric factor.

- (9) If biometric comparison is performed centrally, then a separate key SHALL be used for identifying the device.

SUPPLEMENTAL GUIDANCE: Since the main authentication key has not yet been unlocked, a separate key is required for identifying the specific device(s) that the biometric may be used with.

- (10) If biometric comparison is performed centrally, then biometric revocation, referred to as biometric template protection in ISO/IEC 24745, SHALL be implemented.

SUPPLEMENTAL GUIDANCE: Central databases of biometric templates are an attractive target for attackers. The ability to securely revoke biometric factors is required in response to that threat.

- (11) If biometric comparison is performed centrally, all transmission of biometrics SHALL be over the authenticated protected channel.

SUPPLEMENTAL GUIDANCE: Because of the replay potential of biometric data, biometric information needs to be distributed in a manner that minimizes the opportunity for attackers to intercept the data either by eavesdropping on MitM attacks.

- (12) Biometric samples and any biometric data derived from the biometric sample such as a probe produced through signal processing SHALL be zeroized immediately after any training or research data has been derived.

SUPPLEMENTAL GUIDANCE: If the biometric factor is used for any supplemental purpose, it is important that it not be a mechanism for breach of subscribers' biometric data.

n. Authenticator binding refers to the establishment of an association between a specific authenticator and a subscriber's account, enabling the authenticator to be used — possibly in conjunction with other authenticators — to authenticate for that account.

- (1) Authenticators SHALL be bound to subscriber accounts by either issuance by the CSP as part of enrollment or associating a subscriber-provided authenticator that is acceptable to the CSP.

SUPPLEMENTAL GUIDANCE: In the past, many physical authenticators were provided by the CSP. More recently, there has been a trend toward BYO authenticators, which can be both cost-effective for CSPs and convenient for the subscriber. This requirement ensures that such BYO authenticators are subject to approval by the CSP, primarily to ensure that they meet security requirements.

- (2) Throughout the digital identity lifecycle, CSPs SHALL maintain a record of all authenticators that are or have been associated with each identity.

SUPPLEMENTAL GUIDANCE: In order to authenticate subscribers successfully, the CSP needs to maintain a record of authenticators bound to each subscriber's account. In addition, a record of authenticators formerly bound to each account needs to be kept for forensic purposes.

- (3) The CSP or verifier SHALL maintain the information required for throttling authentication attempts.

SUPPLEMENTAL GUIDANCE: In order to successfully support the throttling of authentication attempts (see requirement IA-5.1 (3)), the CSP needs to maintain information on the number of consecutive failed authentication attempts.

- (4) The CSP SHALL also verify the type of user-provided authenticator so verifiers can determine compliance with requirements at each AAL.

SUPPLEMENTAL GUIDANCE: In order to determine compliance with AAL-specific requirements, the CSP needs to reliably determine some authenticator characteristics, such as whether the authenticator is hardware-based, whether it is a single-factor or multi-factor authenticator, and performance characteristics of associated biometric sensors. Mechanisms to do this include attestation certificates from the manufacturer and examination of the authenticator (particularly at account issuance). In the absence of this information, the CSP needs to assume that the authenticator is the weakest type that is consistent with the authentication protocol being used.

- (5) The record created by the CSP SHALL contain the date and time the authenticator was bound to the account.

SUPPLEMENTAL GUIDANCE: For forensic purposes it is useful to have a record of the period of time each authenticator is bound to the subscriber's account.

- (6) When any new authenticator is bound to a subscriber account, the CSP SHALL ensure that the binding protocol and the protocol for provisioning the associated key(s) are done at AAL2.

SUPPLEMENTAL GUIDANCE: If the process of binding an authenticator is not strong enough, an authenticator that is fraudulently bound to the account could be used by an attacker to gain access to a subscriber's account. The authentication factor being bound to the account needs to be included in the authentication process for the session in which the authenticator is bound.

- (7) Protocols for key provisioning SHALL use authenticated protected channels or be performed in person to protect against MitM attacks.

SUPPLEMENTAL GUIDANCE: For the same reasons that MitM attacks are of concern during authentication, they could occur during provisioning, which could result in the binding of an attacker's key to the account rather than the subscriber's key.

- (8) Binding of multi-factor authenticators SHALL require multi-factor authentication (or equivalent) at identity proofing.

SUPPLEMENTAL GUIDANCE: In order to prevent a subscriber with only single-factor authentication from up-leveling to multi-factor, binding of a multi-factor authenticator requires that the subscriber be multi-factor authenticated at the time the new authenticator is bound

- (9) At enrollment, the CSP SHALL bind at least one, and SHOULD bind at least two, physical (something you have) authenticators to the subscriber's online identity, in addition to a memorized secret or one or more biometrics.

SUPPLEMENTAL GUIDANCE: Executive order 13681 requires the use of multi-factor authentication for the release of personal data. Therefore, it is important that the CSP associate sufficient authentication factors at enrollment to make this possible. While all identifying information is self-asserted at IAL1, preservation of online material or an online reputation makes it undesirable to lose control of an account due to the loss of an authenticator. The second authenticator makes it possible to securely recover from an authenticator loss. For this reason, a CSP SHOULD bind at least two physical authenticators to the subscriber's credential at IAL1 as well.

(10) At enrollment, authenticators at AAL2 and IAL2 SHALL be bound to the account.

SUPPLEMENTAL GUIDANCE: In order to support higher identity assurance, correspondingly high authenticator assurance levels are required to ensure the proper use of the identity.

(11) If enrollment and binding are being done remotely and cannot be completed in a single electronic transaction, then the applicant SHALL identify themselves in each new binding transaction by presenting a temporary secret which was either established during a prior transaction, or sent to the applicant's phone number, email address, or postal address of record.

SUPPLEMENTAL GUIDANCE: The issuance or binding of authenticators may occur well after the enrollment process, following adjudication and eligibility determinations. It is necessary to securely associate the applicant that appears for identity proofing with the person appearing for authenticator issuance/binding in order to avoid mis-issuance of authenticators. At this point it is not possible to fully authenticate the applicant, but the use of a temporary secret provides the necessary protection for this one-time transaction.

(12) If enrollment and binding are being done remotely and cannot be completed in a single electronic transaction, then long-term authenticator secrets are delivered to the applicant within a protected session.

SUPPLEMENTAL GUIDANCE: Long-term secrets need to be protected against disclosure while they are sent to the applicant. This applies primarily to symmetric keys, such as for OTP authenticators, that are sent to the applicant by the CSP. "Protected session" in this context refers to an authenticated protected.

(13) If enrollment and binding are being done in person and cannot be completed in a single physical encounter, the applicant SHALL identify themselves in person by either using a secret as described in IA-5 n (12) above, or through use of a biometric that was recorded during a prior encounter.

SUPPLEMENTAL GUIDANCE: The issuance or binding of authenticators may occur well after the enrollment process, following adjudication and eligibility determinations. It is necessary to securely associate the applicant that appears for identity proofing with the person appearing for authenticator issuance/binding in order to avoid mis-issuance of authenticators. At this point it is not possible to fully authenticate the applicant, but the use of a temporary secret provides the necessary protection for this one-time transaction.

(14) If enrollment and binding are being done in person and cannot be completed in a single physical encounter, temporary secrets SHALL NOT be reused.

SUPPLEMENTAL GUIDANCE: The issuance or binding of authenticators may occur well after the enrollment process, following adjudication and eligibility determinations. It is necessary to securely associate the applicant that appears for identity proofing with the person appearing for authenticator issuance/binding in order to avoid mis-issuance of authenticators. A new secret for this purpose is required for each subsequent encounter.

- (15) If enrollment and binding are being done in person and cannot be completed in a single physical encounter and the CSP issues long-term authenticator secrets during a physical transaction, they SHALL be loaded locally onto a physical device that is issued in person to the applicant or delivered in a manner that confirms the address of record.

SUPPLEMENTAL GUIDANCE: To avoid misappropriation of long-term authenticator secrets at enrollment, the CSP is required to load the secrets onto authenticators directly, or deliver them to the new subscriber in a manner that confirms the address of record, typically by sending a short-term secret to that address that the new subscriber uses to obtain the long-term secret.

- (16) Before adding a new authenticator to a subscriber's account, the CSP SHALL first require the subscriber to authenticate at AAL2 (or a higher AAL) at which the new authenticator will be used.

SUPPLEMENTAL GUIDANCE: In order to maintain the significance of AALs and prevent attackers from leveraging lower AAL authentication to gain access to higher AAL resources, subscribers binding additional authenticators need to do so at the maximum AAL at which they will be used.

- (17) If the subscriber's account has only one authentication factor bound to it, the CSP SHALL require the subscriber to authenticate at AAL1 in order to bind an additional authenticator of a different authentication factor.

SUPPLEMENTAL GUIDANCE: This is a special-case, one-time only exception to IA-5(n)(17) to allow a single-factor account not subject to identity proofing (IAL1) to be upgraded to a multi-factor account. This provides a mechanism for such accounts to increase their authentication security.

- (18) If a subscriber loses all authenticators of a factor necessary to complete multi-factor authentication and has been identity proofed at IAL2, that subscriber SHALL repeat the identity proofing process described in IA-12.

SUPPLEMENTAL GUIDANCE: Repeating the identity proofing process is an onerous requirement when a subscriber is no longer able to complete multi-factor authentication, but it is necessary to avoid the security problems typically present in "account recovery" situations. This is the primary reason that the binding of multiple authenticators is recommended, particularly in the case of physical authenticators. The entire identity

proofing process need not be repeated if the CSP has maintained enough records of the evidence presented to repeat the verification phase of identity proofing.

- (19) If a subscriber loses all authenticators of a factor necessary to complete multi-factor authentication and has been identity proofed at IAL2 or IAL3, the CSP SHALL require the claimant to authenticate using a n authenticator of the remaining factor, if any, to confirm binding to the existing identity.

SUPPLEMENTAL GUIDANCE: While use of an authenticator at a different factor is only a single authentication factor (and therefore only AAL1), authentication in conjunction with the repeated identity proofing process provides assurance that the claimant is who they claim to be.

- (20) If the CSP opts to allow binding of a new memorized secret with the use of two physical authenticators, then it requires entry of a confirmation code sent to an address of record.

SUPPLEMENTAL GUIDANCE: Loss of a memorized secret is different from the loss of a physical authenticator because it is not mitigated by the binding of multiple authenticators. This alternate method of associating a new memorized secret may be used by CSPs to avoid the need for repeating identity proofing (Refer to IA-12).

- (21) If the CSP opts to allow binding of a new memorized secret with the use of two physical authenticators, then the confirmation code SHALL consist of at least 6 random alphanumeric characters generated by an approved random bit generator [SP 800-90Ar1].

SUPPLEMENTAL GUIDANCE: The confirmation code is required to have sufficient entropy and to be generated in a manner that cannot be predicted by an attacker.

- (22) If the CSP opts to allow binding of a new memorized secret with the use of two physical authenticators, then the confirmation code SHALL be valid for a maximum of 7 days but MAY be made valid up to 21 days via an exception process to accommodate addresses outside the direct reach of the U.S. Postal Service. Confirmation codes sent by means other than physical mail SHALL be valid for a maximum of 5 minutes.

SUPPLEMENTAL GUIDANCE: The confirmation code has a limited lifetime to mitigate the risk of loss or misappropriation in transit.

o. Session Management: The following requirements apply to applications where a session is maintained between the subscriber and relying party to allow multiple interactions without repeating the authentication event each time.

Once an authentication event has taken place, it is often desirable to allow the subscriber to continue using the application across multiple subsequent interactions without requiring them

to repeat the authentication event. This requirement is particularly true for federation scenarios where the authentication event necessarily involves several components and parties coordinating across a network.

(1) Session Binding Requirements: A session occurs between the software that a subscriber is running — such as a browser, application, or operating system (i.e., the session subject) — and the RP or CSP that the subscriber is accessing (i.e., the session host).

- a. A session is maintained by a session secret which SHALL be shared between the subscriber's software and the service being accessed.

SUPPLEMENTAL GUIDANCE: This secret binds the two ends of the session, allowing the subscriber to continue using the service over time.

- b. The secret SHALL be presented directly by the subscriber's software or possession of the secret SHALL be proven using a cryptographic mechanism.

SUPPLEMENTAL GUIDANCE: The session secret is considered a short-term secret, so direct presentation of a shared secret is permitted, even at AAL2 or AAL3.

- c. The secret used for session binding SHALL be generated by the session host in direct response to an authentication event.

SUPPLEMENTAL GUIDANCE: The session secret needs to be directly associated with authentication so that it isn't inadvertently provided to the wrong session.

- d. A session SHALL NOT be considered at a higher AAL than the authentication event.

SUPPLEMENTAL GUIDANCE: Each session has an associated maximum AAL at which it can be used that is derived from the authentication AAL; this is associated with the session and its secret by the CSP/RP.

- e. Secrets used for session binding SHALL be generated by the session host during an interaction, typically immediately following authentication.

SUPPLEMENTAL GUIDANCE: It is the responsibility of the host (RP/CSP/Verifier) to generate session secrets, not the subscriber.

- f. Secrets used for session binding SHALL be generated by an approved random bit generator [SP 800-90Ar1].

SUPPLEMENTAL GUIDANCE: The use of a high-quality random bit generator is important to ensure that an attacker cannot guess the session secret.

- g. Secrets used for session binding SHALL contain at least 64 bits of entropy.

SUPPLEMENTAL GUIDANCE: The use of a high-quality random bit generator is important to ensure that an attacker cannot guess the session secret.

- h. Secrets used for session binding SHALL be erased or invalidated by the session subject when the subscriber logs out.

SUPPLEMENTAL GUIDANCE: At a minimum, the CSP/RP needs to ensure that the session secret can no longer be used following logout. If possible, the secret should be erased on the subscriber endpoint as well.

- i. Secrets used for session binding SHALL be sent to and received from the device using an authenticated protected channel.

SUPPLEMENTAL GUIDANCE: Session secrets, particularly when directly presented, need to be protected against eavesdropping and MitM attacks. This is typically accomplished using the Transport Level Security (TLS) protocol.

- j. Secrets used for session binding SHALL time out and not be accepted after the times specified in IA-5 j (13) as appropriate for the AAL.

SUPPLEMENTAL GUIDANCE: This requirement is in support of the reauthentication requirements in AAL2-*, AAL3-*, and REAUTH-*. The proper way to ensure that a session is logged out is to invalidate the session secrets associated with that session. A new session secret will need to be generated and associated with any session that is about to be established from the same endpoint.

- k. Secrets used for session binding SHALL NOT be available to insecure communications between the host and subscriber's endpoint.

SUPPLEMENTAL GUIDANCE: User endpoints such as browsers that support both secure and insecure communications typically have mechanisms to flag information (e.g., cookies) that are only available to secure sessions. These mechanisms are required to be used for session management secrets. See also IA-5 o (7).

- l. Authenticated sessions SHALL NOT fall back to an insecure transport, such as from https to http, following authentication.

SUPPLEMENTAL GUIDANCE: In some cases, endpoints supporting https provide, primarily for legacy purposes, the ability to connect via http as well. If not done properly, this can make the site vulnerable to a "downgrade attack" where a session switches from https to http. This must not happen for authenticated sessions. If session secrets are managed properly, this downgrade interferes with the continuity of the session.

- m. URLs or POST content SHALL contain a session identifier that SHALL be verified by the RP to ensure that actions taken outside the session do not affect the protected session.

SUPPLEMENTAL GUIDANCE: Unique session identifiers in the URL or POST content are used to ensure that sessions are not vulnerable to cross-site request forgery (CSRF). Note that the session identifier is separate and different from the session secret; under no circumstances should the session secret be included in a URL.

- n. Browser cookies SHALL be tagged to be accessible only on secure (HTTPS) sessions.

SUPPLEMENTAL GUIDANCE: Browser cookies have an optional “secure” flag to ensure that they are not accidentally transmitted over a non-secure channel. This flag must be set for session secrets.

- o. Browser cookies SHALL be accessible to the minimum practical set of hostnames and paths.

SUPPLEMENTAL GUIDANCE: Browser cookies have a scope parameter that limits the sites from to which the cookie can be sent; this should be specified as specifically as possible to limit access to the session secret as narrowly as practical.

- p. Expiration of browser cookies SHALL NOT be depended upon to enforce session timeouts.

SUPPLEMENTAL GUIDANCE: While browser cookies have an expiration time, enforcement of session timeouts must occur at the RP/CSP and not at the user endpoint. Cookie expiration may, however, be used to limit accumulation of cookies in the browser.

- q. The presence of an OAuth access token SHALL NOT be interpreted by the RP as presence of the subscriber, in the absence of other signals.

SUPPLEMENTAL GUIDANCE: Access tokens, used in federated identity systems, may be valid after the authentication session has ended and the subscriber has left.

(2) Reauthentication Requirements

- a. Continuity of authenticated sessions SHALL be based upon the possession of a session secret issued by the verifier at the time of authentication and optionally refreshed during the session.

SUPPLEMENTAL GUIDANCE: This is a reiteration of requirement IA-5 o (1).

- b. Session secrets SHALL be non-persistent, i.e., they SHALL NOT be retained across a restart of the associated application or a reboot of the host device.

SUPPLEMENTAL GUIDANCE: Session secrets are not to be maintained across a restart of the associated application or a reboot of the host device in order to minimize the likelihood that a misappropriated logged in device can be exploited.

- c. Periodic reauthentication of sessions (at least every 12 hours per session) SHALL be performed to confirm the continued presence of the subscriber at an authenticated session.

SUPPLEMENTAL GUIDANCE: In order to protect against a subscriber leaving a logged-in endpoint, timeouts are defined for session inactivity and overall session length. The timer for these timeouts is reset by a reauthentication transaction. Higher AALs have more stringent (shorter) reauthentication timeouts. Following expiration of the session timer, the subscriber is required to start a new session by authenticating.

- d. A session SHALL NOT be extended past the guidelines in IA-5 o (2) a – j based on presentation of the session secret alone.

SUPPLEMENTAL GUIDANCE: The existence and possession of a session secret does not consider whether the subscriber continued to be in control of the session endpoint. To mitigate this risk, the session secret is only valid for a limited period of time. While the session secret is “something you have”, it is not an authenticator.

- e. Prior to session expiration, the reauthentication time limit SHALL be extended by prompting the subscriber for the authentication factor(s) of a memorized secret or biometric.

SUPPLEMENTAL GUIDANCE: Before the session times out, the subscriber should be given an opportunity to reauthenticate to extend the session. The subscriber may be prompted when an idle timeout is about to expire, to allow them to cause activity and thereby avoid the need to reauthenticate.

Note: At AAL2, a memorized secret or biometric, and not a physical authenticator, is required because the session secret is something you have, and an additional authentication factor is required to continue the session.

- f. If federated authentication is being used, then since the CSP and RP often employ separate session management technologies, there SHALL NOT be any assumption of correlation between these sessions.

SUPPLEMENTAL GUIDANCE: When an RP session expires and the RP requires reauthentication, it is entirely possible that the session at the CSP has not expired and that a new assertion could be generated from this session at the CSP without reauthenticating the user.

- g. An RP requiring reauthentication through a federation protocol SHALL — if possible within the protocol — specify the maximum (see IA-5 j (10)) acceptable authentication age to the CSP.

SUPPLEMENTAL GUIDANCE: In some applications, RPs may require a “fresh” authentication to meet its authentication risk requirements. By specifying maximum age, the RP can proactively request the CSP to obtain a new authentication to meet that requirement.

- h. If federated authentication is being used and an RP has specific authentication age (see IA-5 j [10]) requirements that it has communicated to the CSP, then the CSP SHALL reauthenticate the subscriber if they have not been authenticated within that time period.

SUPPLEMENTAL GUIDANCE: When the RP communicates its authentication freshness requirements to the CSP, the CSP is expected to reauthenticate the subscriber to support a session that meets those requirements.

- i. If federated authentication is being used, the CSP SHALL communicate the authentication event time to the RP to allow the RP to decide if the assertion is sufficient for reauthentication and to determine the time for the next reauthentication event.

SUPPLEMENTAL GUIDANCE: When federation authentication is being used, the authentication assertion from the CSP needs to contain the authentication event time to allow the RP to request reauthentication at an appropriate interval if it has specific authentication age requirements.

DISCUSSION: Authenticators include passwords, cryptographic devices, biometrics, certificates, one-time password devices, and ID badges. Device authenticators include certificates and passwords. Initial authenticator content is the actual content of the authenticator (e.g., the initial password). In contrast, the requirements for authenticator content contain specific criteria or characteristics (e.g., minimum password length). Developers may deliver system components with factory default authentication credentials (i.e., passwords) to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant risk. The requirement to protect individual authenticators may be implemented via control PL-4 or PS-6 for authenticators in the possession of individuals and by controls AC-3, AC-6, and SC-28 for authenticators stored in organizational

systems, including passwords stored in hashed or encrypted formats or files containing encrypted or hashed passwords accessible with administrator privileges.

Systems support authenticator management by organization-defined settings and restrictions for various authenticator characteristics (e.g., minimum password length, validation time window for time synchronous one-time tokens, and number of allowed rejections during the verification stage of biometric authentication). Actions can be taken to safeguard individual authenticators, including maintaining possession of authenticators, not sharing authenticators with others, and immediately reporting lost, stolen, or compromised authenticators. Authenticator management includes issuing and revoking authenticators for temporary access when no longer needed.

Related Controls: AC-3, AC-6, CM-6, IA-2, IA-4, IA-7, IA-8, MA-4, PE-2, PL-4, SC-12, SC-13.

Control Enhancements:

(1) AUTHENTICATOR MANAGEMENT | AUTHENTICATOR TYPES

[Priority 1]

Control:

(a) Memorized Secret Authenticators and Verifiers:

1. Maintain a list of commonly-used, expected, or compromised passwords via API or download from a third party. Update the list quarterly and when organizational passwords are suspected to have been compromised directly or indirectly. Compare current memorized secrets against the list quarterly;
2. Require immediate selection of a new password upon account recovery;
3. Allow user selection of long passwords and passphrases, including spaces and all printable characters;
4. Employ automated tools to assist the user in selecting strong password authenticators;
5. If chosen by the subscriber, memorized secrets SHALL be at least 8 characters in length.

SUPPLEMENTAL GUIDANCE: Memorized secret length is the most reliable metric determining strength against online and offline guessing attacks. The objective is primarily to defend against online attacks (with throttling of guesses) and to provide some protection against offline attacks, with the primary defense for such attacks being secure storage of the verifier.

6. If chosen by the CSP or verifier using an approved random number generator, memorized secrets SHALL be at least 6 characters in length.

SUPPLEMENTAL GUIDANCE: Memorized secret length is the most reliable metric determining strength against online and offline guessing attacks. The objective is primarily to defend against online attacks (with throttling of guesses) and to provide some protection against offline attacks, with the primary defense for such attacks being secure storage of the verifier.

7. Truncation of the secret SHALL NOT be performed.

SUPPLEMENTAL GUIDANCE: Memorized secrets that are longer than expected by the verifier might (but must not) be simply truncated to an acceptable length. This gives a false impression of security to the user if the verifier only checks a subset of the memorized secret.

8. Memorized secret verifiers SHALL NOT permit the subscriber to store a “hint” that is accessible to an unauthenticated claimant.

SUPPLEMENTAL GUIDANCE: The availability of memorized secret hints greatly weakens the strength of memorized secret authenticators.

9. Verifiers SHALL NOT prompt subscribers to use specific types of information (e.g., “What was the name of your first pet?”) when choosing memorized secrets.

SUPPLEMENTAL GUIDANCE: Prompts for specific information (often called Knowledge-based Authentication or Security Questions) encourage use of the same memorized secrets at multiple sites, which causes a vulnerability to “password stuffing” attacks. This guidance applies to account recovery situations as well as normal authentication.

10. When processing requests to establish and change memorized secrets, verifiers SHALL compare the prospective secrets against the list maintained as required by IA-5(1)(a)(1) that contains values known to be commonly used, expected, or compromised.

SUPPLEMENTAL GUIDANCE: The maintenance of a list of common memorized secrets that cannot be used by users protects against online attacks that might otherwise succeed before throttling mechanisms take effect to defend against these attacks. This is an alternative to the use of composition rules (requirements for particular character types, etc.) and can provide more customized protection against common memorized secrets. This list may include, but is not limited to:

- Passwords obtained from previous breach corpuses.
- Dictionary words.
- Repetitive or sequential characters (e.g., ‘aaaaaa’, ‘1234abcd’).
- Context-specific words, such as the name of the service, the username, and derivatives thereof.

11. If a chosen secret is found in the list, the CSP or verifier SHALL advise the subscriber that they need to select a different secret.

SUPPLEMENTAL GUIDANCE: The use of common memorized secrets greatly increases the vulnerability of the account to both online (guessing) and offline (cracking) attacks. This is an alternative to the use of composition rules (requirements for particular character

types, etc.) and can provide more customized protection against common memorized secrets.

12. If a chosen secret is found in the list, the CSP or verifier SHALL provide the reason for rejection.

SUPPLEMENTAL GUIDANCE: When a subscriber chooses a weak memorized secret, it is likely that they will choose another weak memorized secret that may or may not be on the blocklist. In addition to explaining to the user the reason for the rejection of their selection, it is helpful to provide coaching on better choices. Tools like password-strength meters are often useful in this situation.

13. If a chosen secret is found in the list, the CSP or verifier SHALL require the subscriber to choose a different value.

SUPPLEMENTAL GUIDANCE: When a subscriber chooses a weak memorized secret, the memorized secret change process is not complete until the subscriber has chosen a different value.

14. Verifiers SHALL implement a rate-limiting mechanism that effectively limits failed authentication attempts that can be made on the subscriber's account to no more than five.

SUPPLEMENTAL GUIDANCE: Rate limiting restricts the ability of an attacker to make many online guessing attacks on the memorized secret. Other requirements (e.g., minimum length of memorized secrets) depend on the existence of rate limiting, so effective rate limiting is an essential capability. Ideally, a rate limiting mechanism should restrict the attacker as much as possible without creating an opportunity for a denial-of-service attack against the subscriber.

15. Verifiers SHALL force a change of memorized secret if there is evidence of compromise of the authenticator.

SUPPLEMENTAL GUIDANCE: Although requiring routine periodic changes to memorized secrets is not recommended, it is important that verifiers have the capability to prompt memorized secrets on an emergency basis if there is evidence of a possible successful attack.

16. The verifier SHALL use approved encryption when requesting memorized secrets in order to provide resistance to eavesdropping and MitM attacks.

SUPPLEMENTAL GUIDANCE: As defined in Appendix A of the CJIS Security Policy, cryptography is considered approved if it is specified or adopted in a FIPS or NIST recommendation.

17. The verifier SHALL use an authenticated protected channel when requesting memorized secrets in order to provide resistance to eavesdropping and MitM attacks.

SUPPLEMENTAL GUIDANCE: Communication between claimant and verifier is required to be via an encrypted channel that authenticates the verifier to provide confidentiality of the authenticator output and resistance to MitM attacks. This is typically accomplished using the Transport Level Security (TLS) protocol.

18. Verifiers SHALL store memorized secrets in a form that is resistant to offline attacks.

SUPPLEMENTAL GUIDANCE: Storage of memorized secret verifiers in a hashed form that is not readily reversed is a key protection against offline attacks. In no case should a verifier store memorized secrets in cleartext form. Criteria IA-5(1)(a)(20) – (22) provide more detail on how this is done.

19. Memorized secrets SHALL be salted and hashed using a suitable one-way key derivation function.

SUPPLEMENTAL GUIDANCE: Key derivation functions take a password, a salt, and a cost factor as inputs then generate a password hash. Their purpose is to make each password guessing trial by an attacker who has obtained a password hash file expensive and therefore the cost of a guessing attack high or prohibitive. Use of a key derivation with a salt, preferably with a time- and memory-hard key derivation function, provides the best protection against attackers that are able to obtain a copy of the verifier database.

20. The salt SHALL be at least 32 bits in length and be chosen arbitrarily to minimize salt value collisions among stored hashes.

SUPPLEMENTAL GUIDANCE: Salt values need to be large enough to make it impractical for an attacker to precompute hashed verifier values (so called rainbow tables). While rainbow tables are typically quite large, this requirement would increase their size by a factor of about 4.3 billion. If not chosen arbitrarily, the attacker might be able to anticipate the salt values that would be used, which would eliminate much of this advantage.

21. Both the salt value and the resulting hash SHALL be stored for each subscriber using a memorized secret authenticator

SUPPLEMENTAL GUIDANCE: In order to verify a memorized secret, it needs to be salted and hashed for comparison with the stored verifier (resulting hash). To do this, the salt value needs to be available, and since it is different for each user, needs to be stored with the verifier. It is impractical to verify a memorized secret if this is not done.

22. If an additional iteration of a key derivation function using a salt value known only to the verifier is performed, then this secret salt value SHALL be generated with an approved random bit generator and of sufficient length.

SUPPLEMENTAL GUIDANCE: An additional keyed hashing iteration using a key value that is secret and stored separately from the verifiers provides excellent protection against even attackers (“password crackers”) with substantial computing resources, provided the key is not also compromised. Accordingly, it is important that this salt, which is common to multiple users, be generated in a manner that is not vulnerable to compromise.

23. If an additional iteration of a key derivation function using a salt value known only to the verifier is performed, then this secret salt value SHALL provide at least the minimum-security strength.

SUPPLEMENTAL GUIDANCE: An additional keyed hashing iteration using a key value that is secret and stored separately from the verifiers provides excellent protection against even attackers (“password crackers”) with substantial computing resources, provided the key is not also compromised. Accordingly, it is important that this salt, which is common to multiple users, be of sufficient size to make cryptographic and brute-force attacks impractical.

Currently, the requirement is that the key be at least 112 bits in length.

24. If an additional iteration of a key derivation function using a salt value known only to the verifier is performed, then this secret salt value SHALL be stored separately from the memorized secrets.

SUPPLEMENTAL GUIDANCE: An additional keyed hashing iteration using a key value that is secret and stored separately from the verifiers provides excellent protection against even attackers (“password crackers”) with substantial computing resources, provided the key is not also compromised. Accordingly, it is important that this salt, which is common to multiple users, be stored separately so that it is unlikely to be compromised along with the verifier database. One way to do this is to perform this last hashing iteration on a physically separate processor, since it only requires a value to hash as input and provides the hashed value in response.

DISCUSSION: Password-based authentication applies to passwords regardless of whether they are used in single-factor or multi-factor authentication. Long passwords or passphrases are preferable over shorter passwords. Enforced composition rules provide marginal security benefits while decreasing usability. However, organizations may choose to establish certain rules for password generation (e.g., minimum character length for long passwords) under certain circumstances and can enforce this requirement in IA-5(1)(a)(5). Account recovery can occur, for example, in situations when a password is forgotten. Cryptographically protected passwords include salted one-way cryptographic hashes of passwords. The list of commonly used, compromised, or expected passwords includes passwords obtained from previous breach corpuses,

dictionary words, and repetitive or sequential characters. The list includes context-specific words, such as the name of the service, username, and derivatives thereof.

(b) Look-Up Secret Authenticators and Verifiers

1. CSPs creating look-up secret authenticators SHALL use an approved random bit generator to generate the list of secrets.

SUPPLEMENTAL GUIDANCE: The use of a high-quality random bit generator is important to ensure that an attacker cannot guess the look-up secret

2. Look-up secrets SHALL have at least 20 bits of entropy.

SUPPLEMENTAL GUIDANCE: Look-up secrets need to have enough entropy to ensure that brute-force guessing attacks do not succeed.

3. If look-up secrets are distributed online, then they SHALL be distributed over a secure channel in accordance with the post-enrollment binding requirements in IA-5 'n' 17 through 25.

SUPPLEMENTAL GUIDANCE: Look-up secrets need to be distributed in a manner that minimizes the opportunity for attackers to intercept the secrets either by eavesdropping or MitM attacks.

4. Verifiers of look-up secrets SHALL prompt the claimant for the next secret from their authenticator or for a specific (e.g., numbered) secret.

SUPPLEMENTAL GUIDANCE: In most cases claimants will be prompted for the next unused memorized secret in a list but may be challenged to use a specific secret from a list.

5. A given secret from an authenticator SHALL be used successfully only once.

SUPPLEMENTAL GUIDANCE: Many threats, such as key logging, are enabled if the look-up secret can be used more than once.

6. If a look-up secret is derived from a grid (bingo) card, then each cell of the grid SHALL be used only once.

SUPPLEMENTAL GUIDANCE: Grid (bingo) cards are sometimes used to provide a rudimentary challenge-response authentication involving the claimant. However, an attacker such as a key logger that has persistent access to the endpoint can derive the contents of the grid, and potentially authenticate successfully, if grid entries are reused in subsequent authentication transactions.

Absent the ability to reuse grid squares, grid (bingo) cards will probably no longer be attractive as authenticators.

7. Verifiers SHALL store look-up secrets in a form that is resistant to offline attacks.

SUPPLEMENTAL GUIDANCE: Storage of look-up secret verifiers in a hashed form that is not readily reversed is a key protection against offline attacks. In no case should a verifier store look-up secrets in cleartext form.

8. If look-up secrets have at least 112 bits of entropy, then they SHALL be hashed with an approved one-way function

SUPPLEMENTAL GUIDANCE: Use of an approved one-way function effectively protects the look-up secrets from disclosure if the verifier is compromised. Salting of secrets with this amount of entropy is not required because it is not practical to mount brute-force or cryptographic attacks against secrets this large.

9. If look-up secrets have less than 112 bits of entropy, then they SHALL be salted and hashed using a suitable one-way key derivation function.

SUPPLEMENTAL GUIDANCE: Key derivation functions take a look-up secret, a salt, and a cost factor as inputs then generate a hash. Their purpose is to make each look-up secret guessing trial by an attacker who has obtained a look-up secret hash file expensive and therefore the cost of a guessing attack high or prohibitive. Use of a key derivation with a salt, preferably with a time- and memory-hard key derivation function, provides the best protection against attackers that are able to obtain a copy of the verifier database.

10. If look-up secrets have less than 112 bits of entropy, then the salt SHALL be at least 32 bits in length and be chosen arbitrarily to minimize salt value collisions among stored hashes.

SUPPLEMENTAL GUIDANCE: Salt values need to be large enough to make it impractical for an attacker to precompute hashed verifier values (so called rainbow tables). While rainbow tables are typically quite large, this requirement would increase their size by a factor of about 4.3 billion. If not chosen arbitrarily, the attacker might be able to anticipate the salt values that would be used, which would eliminate much of this advantage.

11. If look-up secrets have less than 112 bits of entropy, then both the salt value and the resulting hash SHALL be stored for each look-up secret.

SUPPLEMENTAL GUIDANCE: In order to verify a look-up secret, it needs to be salted and hashed for comparison with the stored verifier (resulting hash). To do this, the salt value needs to be available, and since it is different for each secret, needs to be stored with the verifier. It is impractical to verify a look-up secret if this is not done.

12. If look-up secrets that have less than 64 bits of entropy, then the verifier SHALL implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber's account.

SUPPLEMENTAL GUIDANCE: Rate limiting restricts the ability of an attacker to make many online guessing attacks on the look-up secret. Other requirements (e.g., minimum length of look-up secrets) depend on the existence of rate limiting, so effective rate limiting is an essential capability. Ideally, a rate limiting mechanism should restrict the attacker as much as possible without creating an opportunity for a denial-of-service attack against the subscriber.

13. The verifier SHALL use approved encryption when requesting look-up secrets in order to provide resistance to eavesdropping and MitM attacks.

SUPPLEMENTAL GUIDANCE: Cryptography is considered approved if it is specified or adopted in a FIPS or NIST recommendation.

14. The verifier SHALL use an authenticated protected channel when requesting look-up secrets in order to provide resistance to eavesdropping and MitM attacks.

SUPPLEMENTAL GUIDANCE: Communication between claimant and verifier is required to be via an encrypted channel that authenticates the verifier to provide confidentiality of the authenticator output and resistance to MitM attacks. This is typically accomplished using the Transport Level Security (TLS) protocol.

(c) Out-of-Band Authenticators and Verifiers

1. The out-of-band authenticator SHALL establish a separate channel with the verifier in order to retrieve the out-of-band secret or authentication request.

SUPPLEMENTAL GUIDANCE: A channel is considered to be out-of-band with respect to the primary communication channel (even if it terminates on the same device) provided the device does not leak information from one channel to the other without the authorization of the claimant.

2. Communication over the secondary channel SHALL be encrypted unless sent via the public switched telephone network (PSTN).

SUPPLEMENTAL GUIDANCE: The secondary channel requires protection to ensure that authentication secrets are not leaked to attackers. Legacy use of the PSTN as an OOB authentication medium is exempt from this requirement, although other requirements apply.

3. Methods that do not prove possession of a specific device, such as voice-over-IP (VoIP) or email, SHALL NOT be used for out-of-band authentication.

SUPPLEMENTAL GUIDANCE: Communication with VoIP phone numbers and email do not establish the possession of a specific device, so they are not suitable for use in out-of-band authentication which is used as a physical authenticator (something you have).

4. If PSTN is not being used for out-of-band communication, then the out-of-band authenticator SHALL uniquely authenticate itself by establishing an authenticated protected channel with the verifier.

SUPPLEMENTAL GUIDANCE: Communication between out-of-band device and verifier is required to be via an encrypted channel to provide confidentiality of the authenticator output and resistance to MitM attacks. This is typically accomplished using the Transport Level Security (TLS) protocol.

5. If PSTN is not being used for out-of-band communication, then the out-of-band authenticator SHALL communicate with the verifier using approved cryptography.

SUPPLEMENTAL GUIDANCE: Cryptography is considered approved if it is specified or adopted in a FIPS or NIST recommendation.

6. If PSTN is not being used for out-of-band communication, then the key used to authenticate the out-of-band device SHALL be stored in suitably secure storage available to the authenticator application (e.g., keychain storage, TPM, TEE, secure element).

SUPPLEMENTAL GUIDANCE: The secret key associated with an out-of-band device or authenticator application is critical to the determination of “something you have” and needs to be well protected.

7. If the PSTN is used for out-of-band authentication and a secret is sent to the out-of-band device via the PSTN, then the out-of-band authenticator SHALL uniquely authenticate itself to a mobile telephone network using a SIM card or equivalent that uniquely identifies the device.

SUPPLEMENTAL GUIDANCE: Since the PSTN does not support the establishment of authenticated protected channels, the alternative method of authenticating the device via the PSTN is supported. Note that there are other specific requirements for use of the PSTN that also apply (see IA-5 (1) c (19) through (20)).

8. If the out-of-band authenticator sends an approval message over the secondary communication channel, it SHALL either accept transfer of a secret from the primary channel to be sent to the verifier via the secondary communications channel, or present a secret received via the secondary channel from the verifier and prompt the claimant to verify the consistency of that secret with the primary channel, prior to accepting a yes/no response from the claimant which it sends to the verifier.

SUPPLEMENTAL GUIDANCE: Most out-of-band verifiers operate by sending a secret over the secondary channel that the subscriber transfers to the primary channel (e.g., the capability to copy and paste from one app to another). Other methods are possible, however, specifically transferring from primary to secondary and user comparison of secrets sent to both channels (with approval being sent to the verifier over the secondary channel). It is good practice to display descriptive information relating to the authentication on the claimant's out-of-band device, to provide additional assurance that the transaction being approved by the subscriber is the correct one, and not from an attacker who exploits the subscriber's approval.

9. The verifier SHALL NOT store the identifying key itself, but SHALL use a verification method (e.g., an approved hash function or proof of possession of the identifying key) to uniquely identify the authenticator.

SUPPLEMENTAL GUIDANCE: In order for the out-of-band authenticator to be considered "something you have", it must be securely authenticated as a unique device or instance of a software-based authentication application. This is required to be done through proof of possession of a key by the authenticator, rather than presentation of the key itself. This provides verifier compromise resistance with respect to the authentication key.

10. Depending on the type of out-of-band authenticator, one of the following SHALL take place: transfer of a secret to the primary channel, transfer of a secret to the secondary channel, or verification of secrets by the claimant.

SUPPLEMENTAL GUIDANCE: Three different methods of associating the primary and secondary channel sessions are permitted. The intent of these methods is to establish approval for a specific authentication transaction, and to minimize the likelihood that an attacker with knowledge of when the subscriber authenticates can obtain approval for a rogue authentication.

11. If the out-of-band authenticator operates by transferring the secret to the primary channel, then the verifier SHALL transmit a random secret to the out-of-band authenticator and then wait for the secret to be returned on the primary communication channel.

SUPPLEMENTAL GUIDANCE: This is the most common form of out-of-band authentication where an authentication secret is transmitted to the out-of-band device and entered by the user for transmission on the primary channel.

12. If the out-of-band authenticator operates by transferring the secret to the secondary channel, then the verifier SHALL display a random authentication secret to the claimant via the primary channel and then wait for the secret to be returned on the secondary channel from the claimant's out-of-band authenticator.

SUPPLEMENTAL GUIDANCE: This is a less typical authentication flow but is also acceptable in that the secret securely associates possession and control of the out-of-band authenticator with the session being authenticated.

13. If the out-of-band authenticator operates by verification of secrets by the claimant, then the verifier SHALL display a random authentication secret to the claimant via the primary channel, send the same secret to the out-of-band authenticator via the secondary channel for presentation to the claimant, and then wait for an approval (or disapproval) message via the secondary channel.

SUPPLEMENTAL GUIDANCE: This is a somewhat more user-friendly authentication flow because it does not require the claimant to read and manually enter the authentication secret, but it carries the additional risk that the claimant will approve the authentication without actually comparing the secrets received from the independent channels. Approval is required to be obtained from the out-of-band authenticator rather than the primary channel because that at least establishes control of the authenticator.

14. The authentication SHALL be considered invalid if not completed within 10 minutes.

SUPPLEMENTAL GUIDANCE: Secrets used in out-of-band authentication are short-term secrets and need to have a definite lifetime. This requirement also relieves the verifier from the responsibility of long-term storage of the secrets.

15. Verifiers SHALL accept a given authentication secret only once during the validity period.

SUPPLEMENTAL GUIDANCE: In order to prevent an attacker who gains access to an authentication secret generated by the subscriber from using it, it is important that the secret only be valid for a single authentication. This requirement only applies when a secret is being transferred between the primary channel and the out-of-band authenticator.

16. The verifier SHALL generate random authentication secrets with at least 20 bits of entropy.

SUPPLEMENTAL GUIDANCE: Consistent with other short-term authentication secrets, 20 bits of entropy are required to provide resistance against brute force attacks. 6-digit numeric secrets (19.93 bits of entropy) are sufficiently close to 20 bits to be acceptable.

17. The verifier SHALL generate random authentication secrets using an approved random bit generator.

SUPPLEMENTAL GUIDANCE: The use of a high-quality random bit generator is important to ensure that an attacker cannot guess the out-of-band secret. Approved random bit generators are generally included in a FIPS 140-2 certified encryption module.

18. If the authentication secret has less than 64 bits of entropy, the verifier SHALL implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber's account as described in IA-5 l (3) through (4).

SUPPLEMENTAL GUIDANCE: Rate limiting limits the opportunity for attackers to mount a brute-force attack on the out-of-band verifier. Since the out-of-band secret has a limited lifetime, it is sufficient to limit the number of attempts allowed during the (maximum) 10-minute lifetime of the secret.

19. If out-of-band verification is to be made using the PSTN, then the verifier SHALL verify that the pre-registered telephone number being used is associated with a specific physical device.

SUPPLEMENTAL GUIDANCE: Some telephone numbers, such as those that are associated with VoIP services, are not associated with a specific device and can receive calls and text messages without establishing possession and control of a specific device. Such telephone numbers are not suitable for OOB authentication. Services exist to distinguish telephone numbers that are associated with a device from those that aren't.

20. If out-of-band verification is to be made using the PSTN, then changing the pre-registered telephone number is considered to be the binding of a new authenticator and SHALL only occur as described in IA-5 n (17) through (25).

SUPPLEMENTAL GUIDANCE: The binding of a new authenticator requires that the subscriber authenticate at the same or a higher AAL (currently AAL2) than that at which the authenticator will be used, and that a notification be sent to the subscriber. This is required to prevent attackers from changing the phone number of a PSTN-based out-of-band authenticator to one they control.

21. If PSTN is used for out-of-band authentication, then the CSP SHALL offer subscribers at least one alternate authenticator that is not RESTRICTED and can be used to authenticate at the required AAL.

SUPPLEMENTAL GUIDANCE: Use of the PSTN for out-of-band authentication involves additional risk, resulting in its being designated as a restricted authenticator. CSPs are required to provide subscribers with a meaningful alternative.

22. If PSTN is used for out-of-band authentication, then the CSP SHALL Provide meaningful notice to subscribers regarding the security risks of the RESTRICTED authenticator and availability of alternative(s) that are not RESTRICTED.

SUPPLEMENTAL GUIDANCE: Use of the PSTN for out-of-band authentication involves additional risk, resulting in its being designated as a restricted authenticator. CSPs are required to explain these risks to subscribers and offer more secure alternatives.

Currently, authenticators leveraging the public switched telephone network, including phone- and Short Message Service (SMS)-based one-time passwords (OTPs) are restricted. Other authenticator types may be added as additional threats emerge. Note that, among other requirements, even when using phone- and SMS-based OTPs, the agency also must verify that the OTP is being directed to a phone and not an IP address, such as with VoIP, as these accounts are not typically protected with multi-factor authentication.

23. If PSTN is used for out-of-band authentication, then the CSP SHALL address any additional risk to subscribers in its risk assessment.

SUPPLEMENTAL GUIDANCE: Use of the PSTN for out-of-band authentication involves additional risk, resulting in its being designated as a restricted authenticator. These risks need to be documented.

24. If PSTN is used for out-of-band authentication, then the CSP SHALL develop a migration plan for the possibility that the RESTRICTED authenticator is no longer acceptable at some point in the future and include this migration plan in its digital identity acceptance statement.

SUPPLEMENTAL GUIDANCE: Use of the PSTN for out-of-band authentication involves additional risk, resulting in its being designated as a restricted authenticator. A plan for eliminating them in the future needs to be documented.

(d) OTP Authenticators and Verifiers

1. The secret key and its algorithm SHALL provide at least the minimum security strength of 112 bits as of the date of this publication.

SUPPLEMENTAL GUIDANCE: The secret key used by an OTP authenticator needs to be sufficiently complex to resist online and offline attacks. An attacker may have the ability to observe the authenticator output at some point during its operation; it needs to be impractical for the secret key to be derived from a set of these observations.

2. The nonce SHALL be of sufficient length to ensure that it is unique for each operation of the device over its lifetime.

SUPPLEMENTAL GUIDANCE: If the nonce isn't long enough, the output of the authenticator will repeat, which represents an easily avoided vulnerability.

3. OTP authenticators — particularly software-based OTP generators — SHALL NOT facilitate the cloning of the secret key onto multiple devices.

SUPPLEMENTAL GUIDANCE: Like other physical authenticators, the use of OTP authenticators is premised upon the authenticator secret being present in a single authenticator so that it proves possession of a specific device. Mechanisms that would facilitate cloning the secret onto multiple devices include the ability to enroll more than one device producing the same OTP output and backup mechanisms, especially when software-based authenticators are used. Verifiers are expected to make their best effort at determining that bring-your-own authenticators not issued by them meet this requirement and to have policies not allowing the use of non-compliant authenticators.

4. The authenticator output SHALL have at least 6 decimal digits (approximately 20 bits) of entropy.

SUPPLEMENTAL GUIDANCE: Consistent with other short-term authentication secrets, 20 bits of entropy are required to provide resistance against brute force attacks. 6-digit numeric secrets (19.93 bits of entropy) are sufficiently close to 20 bits to be acceptable.

5. If the nonce used to generate the authenticator output is based on a real-time clock, then the nonce SHALL be changed at least once every 2 minutes.

SUPPLEMENTAL GUIDANCE: The authenticator output needs to be changed often enough that there is reasonable assurance that it is in the possession of the claimant and that it is not susceptible to OTP-guessing attacks.

6. The OTP value associated with a given nonce SHALL be accepted only once.

SUPPLEMENTAL GUIDANCE: A fundamental premise of a “one-time” authenticator is that it can be used successfully only once during its validity period.

7. The symmetric keys used by authenticators are also present in the verifier and SHALL be strongly protected against compromise.

SUPPLEMENTAL GUIDANCE: Verifiers typically contain symmetric keys for all subscribers using OTP authenticators. This makes them a particularly rich target for attackers. While the protection of these keys is implementation-dependent and there is therefore no specific requirement for how the keys are protected, measures to prevent the exfiltration of the keys are needed. An example of such a measure is the storage of keys and generation of authenticator outputs in a separate device accessible only by the verifier.

8. If a single-factor OTP authenticator is being associated with a subscriber account, then the verifier or associated CSP SHALL use approved cryptography to either generate and exchange or to obtain the secrets required to duplicate the authenticator output.

SUPPLEMENTAL GUIDANCE: It is critical that authentication secrets be generated and transferred or negotiated securely. This includes the use of secure random number generators and protocols for transferring or negotiating (e.g., Diffie-Hellman) secret values.

Cryptography is considered approved if it is specified or adopted in a FIPS or NIST recommendation.

9. The verifier SHALL use approved encryption when collecting the OTP.

SUPPLEMENTAL GUIDANCE: Cryptography is considered approved if it is specified or adopted in a FIPS or NIST recommendation.

10. The verifier SHALL use an authenticated protected channel when collecting the OTP.

SUPPLEMENTAL GUIDANCE: Communication between claimant and verifier is required to be via an encrypted channel that authenticates the verifier to provide confidentiality of the authenticator output and resistance to MitM attacks. This is typically accomplished using the Transport Level Security (TLS) protocol.

11. If a time-based OTP is used, it SHALL have a defined lifetime (recommended 30 seconds) that is determined by the expected clock drift — in either direction — of the authenticator over its lifetime, plus allowance for network delay and user entry of the OTP.

SUPPLEMENTAL GUIDANCE: The clocks on time-based authenticators are subject to drift because of cost and environmental factors such as temperature. Accordingly, verifiers need to accept authenticator outputs before and particularly after the intended validity period to allow use by authenticators that are not in synchronization.

12. Verifiers SHALL accept a given time-based OTP only once during the validity period.

SUPPLEMENTAL GUIDANCE: In order to prevent an attacker who gains access to an OTP authenticator output from using it, it is important that the secret only be valid for a single authentication.

13. If the authenticator output has less than 64 bits of entropy, the verifier SHALL implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber's account as described in IA-5 l (3) through (4).

SUPPLEMENTAL GUIDANCE: OTPs whose output has less entropy are more vulnerable to online guessing attacks. To mitigate these attacks, rate limiting is required. Online guessing attacks are less of a concern for time-based OTP authenticators because of the limited validity window, but a limit on the number of guesses during a given validity period is effective in resisting automated attacks.

14. If the authenticator is multi-factor, then each use of the authenticator SHALL require the input of the additional factor.

SUPPLEMENTAL GUIDANCE: To ensure that a multi-factor authenticator cannot be stolen and used repeatedly following activation, a separate activation is required for each use of the authenticator. It is preferable for a multi-factor authenticator not to indicate that the wrong memorized secret or biometric were presented, but rather to produce an authenticator output that is invalid, although this is not required. This provides protection against guessing or presentation attacks on the authenticator itself.

15. If the authenticator is multi-factor and a memorized secret is used by the authenticator for activation, then that memorized secret SHALL be a randomly chosen numeric secret at least 6 decimal digits in length or other memorized secret meeting the requirements of IA-5 (1)(a).

SUPPLEMENTAL GUIDANCE: The requirement for memorized secrets used as activation factors is the same as that for memorized secrets used as distinct authenticators (see IA-5 (1)(a)).

16. If the authenticator is multi-factor, then use of a memorized secret for activation SHALL be rate limited as specified in IA-5 l (3) through (4).

SUPPLEMENTAL GUIDANCE: Rate limiting is required to provide protection against brute-force guessing attacks, particularly if the authenticator gives an indication when an incorrect secret is entered.

17. If the authenticator is multi-factor and is activated by a biometric factor, then that factor SHALL meet the requirements of IA-5 m, including limits on the number of consecutive authentication failures.

SUPPLEMENTAL GUIDANCE: General requirements for biometric activation factors include false accept rate criteria and the number of consecutive authentication failures that are allowed.

18. If the authenticator is multi-factor, then the unencrypted key and activation secret or biometric sample — and any biometric data derived from the biometric sample such as a probe produced through signal processing — SHALL be zeroized immediately after an OTP has been generated.

SUPPLEMENTAL GUIDANCE: It is important that the unencrypted key and associated data be zeroized to minimize the likelihood that it can be misappropriated by an attacker following a successful authentication. Each authentication requires a re-presentation of the activation factor (see IA-5(1)(d)14). Verifiers are expected to make their best effort at determining that bring-your-own authenticators not issued by them meet this requirement and to have policies not allowing the use of non-compliant authenticators.

19. If the authenticator is multi-factor, the verifier or CSP SHALL establish, via the authenticator source, that the authenticator is a multi-factor device.

SUPPLEMENTAL GUIDANCE: From the standpoint of a verifier, a multi-factor OTP authenticator appears the same as a single-factor OTP authenticator. In order to establish that the authenticator meets the multi-factor requirements, the verifier or CSP can issue the authenticator, examine it in some way, or rely on an assertion from the manufacturer.

20. In the absence of a trusted statement that it is a multi-factor device, the verifier SHALL treat the authenticator as single-factor, in accordance with IA-5 (1) (d) (1) through (13).

SUPPLEMENTAL GUIDANCE: Authenticators of unknown provenance or that are not known by the CSP or verifier to meet all of the requirements for multi-factor OTP authenticators can be used, but only as single-factor authenticators.

(e) Cryptographic Authenticators and Verifiers (including single- and multi-factor cryptographic authenticators, both hardware- and software-based)

1. If the cryptographic authenticator is software based, the key SHALL be stored in suitably secure storage available to the authenticator application.

SUPPLEMENTAL GUIDANCE: Although dependent on the computing device on which the authenticator is operating, authenticator software needs to avail itself of the most secure storage available, considering issues like ability to extract the secret from the device and its potential to be included in backup data. Verifiers are expected to make their best effort at determining that bring-your-own authenticators not issued by them meet this requirement and to have policies not allowing the use of non-compliant authenticators.

2. If the cryptographic authenticator is software based, the key SHALL be strongly protected against unauthorized disclosure by the use of access controls that limit access to the key to only those software components on the device requiring access.

SUPPLEMENTAL GUIDANCE: Although dependent on the computing device on which the authenticator is operating, authenticator software needs to store secret keys in a manner that limits access to keys to the maximum extent possible so that they cannot be accessed by other (possibly rogue) applications and/or users. Verifiers are expected to make their best effort at determining that bring-your-own authenticators not issued by them meet this requirement and to have policies not allowing the use of non-compliant authenticators.

3. If the cryptographic authenticator is software based, it SHALL NOT facilitate the cloning of the secret key onto multiple devices.

SUPPLEMENTAL GUIDANCE: Like other physical authenticators, the use of cryptographic authenticators is premised upon the authenticator secret being present in a single authenticator so that it proves possession of a specific device. Mechanisms that would facilitate cloning the secret onto multiple devices include the ability to enroll more

than one device with the same key and backup mechanisms, especially when software-based authenticators are used. Verifiers are expected to make their best effort at determining that bring-your-own authenticators not issued by them meet this requirement and to have policies not allowing the use of non-compliant authenticators.

4. If the authenticator is single-factor and hardware-based, secret keys unique to the device SHALL NOT be exportable (i.e., cannot be removed from the device).

SUPPLEMENTAL GUIDANCE: Cryptographic device authenticators are constructed so as not to allow the secret key to be obtained from the device. These devices are enrolled for authentication using the public cryptographic key, but the private key is never shared. This requirement addresses primarily functionality allowing the key to be exported; FIPS 140 requirements cover the resistance of the device to various forms of attack.

5. If the authenticator is hardware-based, the secret key and its algorithm SHALL provide at least the minimum-security length of 112 bits as of the date of this publication.

SUPPLEMENTAL GUIDANCE: The secret key used by a cryptographic authenticator needs to be sufficiently complex to resist online and offline attacks. An attacker may have the ability to observe the authenticator output at some point during its operation; it needs to be impractical for the secret key to be derived from a set of these observations. Since verifiers and cryptographic authenticators must use the same algorithms to successfully authenticate, assessment of the verifier also assesses the authenticators that may be used.

6. If the authenticator is hardware-based, the challenge nonce SHALL be at least 64 bits in length.

SUPPLEMENTAL GUIDANCE: This requirement applies to hardware-based cryptographic authenticators. The challenge nonce is required to be large enough that it will not be reused during the lifetime of the authenticator in order to provide replay protection. Since verifiers and cryptographic authenticators must use the same algorithms to successfully authenticate, assessment of the nonce generated by the verifier also assesses the authenticators that may be used.

7. If the authenticator is hardware-based, approved cryptography SHALL be used.

SUPPLEMENTAL GUIDANCE: Cryptography is considered approved if it is specified or adopted in a FIPS or NIST recommendation. Since verifiers and cryptographic authenticators must use the same algorithms to successfully authenticate, assessment of the verifier also assesses the authenticators that may be used.

8. Cryptographic keys stored by the verifier SHALL be protected against modification.

SUPPLEMENTAL GUIDANCE: Protection against modification is required for all keys to ensure that an attacker can't substitute keys they control, which would permit them to

authenticate successfully. This protection could be provided by operating system access controls, or through integrity checks of the stored keys with separately stored hashes.

9. If symmetric keys are used, cryptographic keys stored by the verifier SHALL be protected against disclosure.

SUPPLEMENTAL GUIDANCE: Protection against disclosure is required for symmetric keys because their disclosure also would permit an attacker to authenticate successfully. This protection could be provided through operating system access controls.

10. The challenge nonce SHALL be at least 64 bits in length.

SUPPLEMENTAL GUIDANCE: This requirement applies to verifiers of cryptographic authentication. The challenge nonce is generated by the verifier and used by a cryptographic authenticator to compute the authenticator output. The challenge needs to be sufficiently long that it will not need to repeat during the lifetime of the authenticator, so the authenticator output, if available to an attacker, cannot be replayed.

11. The challenge nonce SHALL either be unique over the authenticator's lifetime or statistically unique (i.e., generated using an approved random bit generator).

SUPPLEMENTAL GUIDANCE: The challenge nonce is generated by the verifier used by a cryptographic authenticator to compute the authenticator output. The nonce cannot repeat during the lifetime of the authenticator, so the authenticator output, if available to an attacker, cannot be replayed. This can be accomplished by either deterministic means (e.g., an algorithm choosing values guaranteed not to repeat) or statistically (random values chosen from a range giving a very low probability that the same nonce will ever be seen twice).

12. The verification operation SHALL use approved cryptography.

SUPPLEMENTAL GUIDANCE: Cryptography is considered approved if it is specified or adopted in a FIPS or NIST recommendation. Since verifiers and cryptographic authenticators must use the same algorithms to successfully authenticate, assessment of the verifier also assesses the authenticators that may be used.

13. If a multi-factor cryptographic software authenticator is being used, then each authentication requires the presentation of the activation factor.

SUPPLEMENTAL GUIDANCE: The activation factor, either a memorized secret or a biometric, is required to be presented each time an authentication operation is requested by the authenticator to ensure that an activated authenticator cannot be used by an attacker.

14. If the authenticator is multi-factor, then any memorized secret used by the authenticator for activation SHALL be a randomly chosen numeric secret at least 6 decimal digits in length or other memorized secret meeting the requirements of IA-5 (1) (a).

SUPPLEMENTAL GUIDANCE: The requirement for memorized secrets used as activation factors is the same as that for memorized secrets used as distinct authenticators (see IA-5(1)a).

15. If the authenticator is multi-factor, then use of a memorized secret for activation SHALL be rate limited as specified in IA-5 l (3) through (4).

SUPPLEMENTAL GUIDANCE: Rate limiting is required to provide protection against brute-force guessing attacks, particularly if the authenticator gives an indication when an incorrect secret is entered.

16. If the authenticator is multi-factor and is activated by a biometric factor, then that factor SHALL meet the requirements of IA-5 m, including limits on the number of consecutive authentication failures.

SUPPLEMENTAL GUIDANCE: General requirements for biometric activation factors include false accept rate criteria and the number of consecutive authentication failures that are allowed.

17. If the authenticator is multi-factor, then the unencrypted key and activation secret or biometric sample — and any biometric data derived from the biometric sample such as a probe produced through signal processing — SHALL be zeroized immediately after an authentication transaction has taken place.

SUPPLEMENTAL GUIDANCE: It is important that the unencrypted key and associated data be zeroized to minimize the likelihood that it can be misappropriated by an attacker following a successful authentication. Verifiers are expected to make their best effort at determining that bring-your-own authenticators not issued by them meet this requirement and to have policies not allowing the use of non-compliant authenticators.

Related Controls: IA-6.

Control Enhancements:

(2) AUTHENTICATOR MANAGEMENT | PUBLIC KEY BASED AUTHENTICATION

[Existing] [Priority 1]

Control:

(a) For public key-based authentication:

1. Enforce authorized access to the corresponding private key; and

2. Map the authenticated identity to the account of the individual or group; and
- (b) When public key infrastructure (PKI) is used:
1. Validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; and
 2. Implement a local cache of revocation data to support path discovery and validation.

DISCUSSION: Public key cryptography is a valid authentication mechanism for individuals, machines, and devices. For PKI solutions, status information for certification paths includes certificate revocation lists or certificate status protocol responses. For PIV cards, certificate validation involves the construction and verification of a certification path to the Common Policy Root trust anchor, which includes certificate policy processing. Implementing a local cache of revocation data to support path discovery and validation also supports system availability in situations where organizations are unable to access revocation information via the network. A local cache of revocation data is also known as a certificate revocation list. This list contains a list of revoked certificates and can be periodically downloaded to ensure certificates can still be checked for revocation when network access is not available or access to the Online Certificate Status Protocol (OCSP) server is not available. Without configuring a local cache of revocation data, there is the potential to allow access to users who are no longer authorized (users with revoked certificates).

Related Controls: IA-3, SC-17.

(6) AUTHENTICATOR MANAGEMENT | PROTECTION OF AUTHENTICATORS

[Existing] [Priority 1]

Control:

Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access.

DISCUSSION: For systems that contain multiple security categories of information without reliable physical or logical separation between categories, authenticators used to grant access to the systems are protected commensurate with the highest security category of information on the systems. Security categories of information are determined as part of the security categorization process.

Related Controls: RA-2.

IA-6 AUTHENTICATION FEEDBACK

[Existing] [Priority 3] Control:

Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.

DISCUSSION: Authentication feedback from systems does not provide information that would allow unauthorized individuals to compromise authentication mechanisms. For some types of systems, such as desktops or notebooks with relatively large monitors, the threat (referred to as

shoulder surfing) may be significant. For other types of systems, such as mobile devices with small displays, the threat may be less significant and is balanced against the increased likelihood of typographic input errors due to small keyboards. Thus, the means for obscuring authentication feedback is selected accordingly. Obscuring authentication feedback includes displaying asterisks when users type passwords into input devices or displaying feedback for a very limited time before obscuring it.

Related Controls: AC-3.

IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION

[Priority 2]

Control:

Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.

DISCUSSION: Authentication mechanisms may be required within a cryptographic module to authenticate an operator accessing the module and to verify that the operator is authorized to assume the requested role and perform services within that role.

Related Controls: AC-3, IA-5, SA-4, SC-12, SC-13.

IA-8 IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)

[Priority 2]

Control:

Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.

DISCUSSION: Non-organizational users include system users other than organizational users explicitly covered by IA-2. Non-organizational users are uniquely identified and authenticated for accesses other than those explicitly identified and documented in AC-14. Identification and authentication of non-organizational users accessing federal systems may be required to protect federal, proprietary, or privacy-related information (with exceptions noted for national security systems). Organizations consider many factors—including security, privacy, scalability, and practicality—when balancing the need to ensure ease of use for access to federal information and systems with the need to protect and adequately mitigate risk.

Related Controls: AC-2, AC-6, AC-14, AC-17, AC-18, AU-6, IA-2, IA-4, IA-5, IA-11, MA-4, RA-3, SA-4, SC-8.

Control Enhancements:

(1) IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | ACCEPTANCE OF PIV CREDENTIALS FROM OTHER AGENCIES

[Priority 2]

Control:

Accept and electronically verify Personal Identity Verification-compliant credentials from other federal, state, local, tribal, or territorial (SLTT) agencies.

DISCUSSION: Acceptance of Personal Identity Verification (PIV) credentials from other federal or SLTT agencies applies to both logical and physical access control systems. PIV credentials are those credentials issued by federal or SLTT agencies that conform to FIPS Publication 201 and supporting guidelines.

Related Controls: PE-3.

(2) IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | ACCEPTANCE OF EXTERNAL AUTHENTICATORS

[Priority 2]

Control:

- (a) Accept only external authenticators that are NIST-compliant; and
- (b) Document and maintain a list of accepted external authenticators.

DISCUSSION: Acceptance of only NIST-compliant external authenticators applies to organizational systems that are accessible to the public (e.g., public-facing websites). External authenticators are issued by nonfederal government entities and are compliant with the CJISSECPOL. Approved external authenticators meet or exceed the minimum Federal Government-wide technical, security, privacy, and organizational maturity requirements. Meeting or exceeding Federal requirements allows Federal Government relying parties to trust external authenticators in connection with an authentication transaction at a specified authenticator assurance level.

Related Controls: None.

(4) IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | USE OF DEFINED PROFILES

[Priority 2]

Control:

Conform to the following profiles for identity management: Security Assertion Markup Language (SAML) or OpenID Connect.

DISCUSSION: Organizations define profiles for identity management based on open identity management standards. To ensure that open identity management standards are viable, robust, reliable, sustainable, and interoperable as documented, the Federal Government assesses and scopes the standards and technology implementations against applicable laws, executive orders, directives, policies, regulations, standards, and guidelines.

Related Controls: None.

IA-11 RE-AUTHENTICATION

[Priority 2]

Control:

Require users to re-authenticate when: roles, authenticators, or credentials change, security categories of systems change, the execution of privileged functions occur, or every 12 hours.

DISCUSSION: In addition to the re-authentication requirements associated with device locks, organizations may require re-authentication of individuals in certain situations, including when roles, authenticators, or credentials change, when security categories of systems change, when the execution of privileged functions occurs, after a fixed time period, or periodically.

Related Controls: AC-3, AC-11, IA-2, IA-3, IA-4, IA-8.

IA-12 IDENTITY PROOFING

[Priority 2]

Control:

- a. Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines;
- b. Resolve user identities to a unique individual; and
- c. Collect, validate, and verify identity evidence.

DISCUSSION: Identity proofing is the process of collecting, validating, and verifying a user's identity information for the purposes of establishing credentials for accessing a system. Identity proofing is intended to mitigate threats to the registration of users and the establishment of their accounts. Organizations may be subject to laws, executive orders, directives, regulations, or policies that address the collection of identity evidence. Organizational personnel consult with the senior agency official for privacy and legal counsel regarding such requirements.

Related Controls: AC-5, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-8.

Control Enhancements:

(2) IDENTITY PROOFING | IDENTITY EVIDENCE

[Priority 2]

Control:

Require evidence of individual identification be presented to the registration authority.

DISCUSSION: Identity evidence, such as documentary evidence or a combination of documents and biometrics, reduces the likelihood of individuals using fraudulent identification to establish an identity or at least increases the work factor of potential adversaries. The forms of acceptable

evidence are consistent with the risks to the systems, roles, and privileges associated with the user's account.

Related Controls: None.

(3) IDENTITY PROOFING | IDENTITY EVIDENCE VALIDATION AND VERIFICATION

[Priority 2]

Control:

- a. Require that the presented identity evidence be validated and verified through agency-defined resolution, validation, and verification methods.

DISCUSSION: Validation and verification of identity evidence increases the assurance that accounts and identifiers are being established for the correct user and authenticators are being bound to that user. Validation refers to the process of confirming that the evidence is genuine and authentic, and the data contained in the evidence is correct, current, and related to an individual. Verification confirms and establishes a linkage between the claimed identity and the actual existence of the user presenting the evidence. Acceptable methods for validating and verifying identity evidence are consistent with the risks to the systems, roles, and privileges associated with the users account.

- b. Identity proofing SHALL NOT be performed to determine suitability or entitlement to gain access to services or benefits.

SUPPLEMENTAL GUIDANCE: The sole objective of identity proofing is to ensure the applicant is who they claim to be to a stated level of certitude.

- c.
 1. Collection of PII SHALL be limited to the minimum necessary to resolve to a unique identity in a given context.

2. Collection of PII SHALL be limited to the minimum necessary to validate the existence of the claimed identity and associate the claimed identity with the applicant providing identity evidence for appropriate identity resolution, validation, and verification.

SUPPLEMENTAL GUIDANCE: The goal of identity resolution is to uniquely distinguish an individual within a given population or context. Effective identity resolution uses the smallest set of attributes necessary to resolve to a unique individual. It provides the CSP an important starting point in the overall identity proofing process, to include the initial detection of potential fraud, but in no way represents a complete and successful identity proofing transaction.

Collection of PII may include attributes are used to correlate identity evidence to authoritative sources and to provide RPs with attributes used to make authorization decisions. There may be many different sets that suffice as the minimum, so it is recommended that CSPs choose this set to balance privacy and the user's usability needs, as well as the likely attributes needed in future uses of the digital identity.

Examples of attributes that may be used for minimum identity attribute sets include:

- Name (first, last, middle) with combinations and variations,
- Address (#, Street, City, County, State, Zip code) with combinations and variations,

- Date of birth (DDMMYYYY) with combinations and variations,
- Email address,
- Phone number.

For population sets that are more defined than the general population (e.g., military veterans, Native Americans), these minimum attribute sets may be tailored to that specific community.

Additionally, it is recommended that CSPs document which alternative attributes it will accept in cases where an applicant cannot provide the minimum necessary attributes (e.g., applicant does not have a home address or phone number).

d. The CSP SHALL provide explicit notice to the applicant at the time of collection regarding the purpose for collecting and maintaining a record of the attributes necessary for identity proofing, including whether such attributes are voluntary or mandatory to complete the identity proofing process, and the consequences for not providing the attributes.

SUPPLEMENTAL GUIDANCE: Notice of proofing may contain at a minimum:

- Attribute information that is mandatory
- Attribute information that is voluntary
- What will be done with the information collected
- How the information will be protected
- Consequence of not providing mandatory attribute information (e.g., suspension/termination of the identity proofing process).

This notice may be delivered as an online screen (for remote identity proofing), a poster or printed notice at in-person proofing locations, or an oral notice delivered at the time of information collection.

e. If CSPs process attributes for purposes other than identity proofing, authentication, or attribute assertions (collectively “identity service”), related fraud mitigation, or to comply with law or legal process, then CSPs SHALL implement measures to maintain predictability and manageability commensurate with the privacy risk arising from the additional processing.

SUPPLEMENTAL GUIDANCE: Predictability and manageability measures include providing clear notice, obtaining subscriber consent, or enabling selective use or disclosure of attributes.

Predictability is meant to build trust and provide accountability and requires full understanding (and disclosure) of how the attribute information will be used. Manageability also builds trust by demonstrating a CSPs ability to control attribute information throughout processing – collection, maintenance, retention.

f. If the CSP employs consent as part of its measures to maintain predictability and manageability, ...then it SHALL NOT make consent for the additional processing a condition of the identity service.

SUPPLEMENTAL GUIDANCE: Consent involves collecting and recording an affirmative response from the applicant that they agree to the additional processing of their attributes. In order to make this consent meaningful, it is recommended that CSPs first disclose to its applicants which attributes are being collected and processed and why.

g. The CSP SHALL provide mechanisms for redress of applicant complaints or problems arising from the identity proofing.

These [redress] mechanisms SHALL be easy for applicants to find and use.

SUPPLEMENTAL GUIDANCE: The Privacy Act requires federal CSPs that maintain a system of records to follow procedures to enable applicants to access and, if incorrect, amend their records. Any Privacy Act Statement should include a reference to the applicable SORN(s), which provide the applicant with instructions on how to make a request for access or correction. It is recommended that non-federal CSPs have comparable procedures, including contact information for any third parties if they are the source of the information.

It is recommended that CSPs make the availability of any alternative methods for completing the identity proofing and enrollment processes clear to users (e.g., in person at a customer service center, if available) in the event an applicant is unable to properly complete the initial identity proofing and enrollment process requirements online.

Note: If the ID proofing process is not successful, it is recommended that CSPs inform the applicant of the procedures to address the issue but avoid informing the applicant of the specifics of why the registration failed.

To be effective, the use of a CSP's redress mechanism results in a timely correction of errors, resolution of the dispute or complaint, and the process should not be overly burdensome or complex.

It is recommended that the CSP document and publish, in a manner which is easy for Applicants to find and use, its mechanisms for redress of Applicant complaints or problems arising from the identity proofing processes.

h. The CSP SHALL assess the [redress] mechanisms for their efficacy in achieving resolution of complaints or problems.

SUPPLEMENTAL GUIDANCE: "Effective" in this requirement means that use of the redress mechanism will result in a timely correction of errors, resolution of the dispute or complaint, and the process shall not be overly burdensome or complex.

It is recommended that CSPs maintain a record or log of all cases – including outcomes – where applicants have sought redress for complaints or problems arising from the identity proofing and provide for the periodic review of these records.

i. The identity proofing and enrollment processes SHALL be performed according to an applicable written policy or *practice statement* that specifies the particular steps taken to verify identities.

SUPPLEMENTAL GUIDANCE: Having documented procedures is a prerequisite for transparency, accountability, quality control, auditability, and ease of interoperability among federated communities. The documentation, dissemination, review and update to identity and authentication processes is a core control under IA-1 Identification and Authentication Policy and Procedures.

j. The *practice statement* SHALL include control information detailing how the CSP handles proofing errors that result in an applicant not being successfully enrolled.

SUPPLEMENTAL GUIDANCE: “Proofing errors” in this context refer to circumstances that result in the inability or failure to complete the identity proofing and enrollment processes. Such circumstances may include:

- Applicant abandons the identity proofing and enrollment processes;
- Applicant fails to provide mandatory attribute information;
- Identity evidence of required strength is not provided;
- Identity evidence is rejected following inspection;
- Identity evidence and information do not correlate;
- Information from identity evidence is not validated by issuing or authoritative sources at the required strength;
- Identity evidence verification of binding to the applicant fails; and
- Applicant fails to confirm enrollment code within code validity period.

Depending on the circumstances above, it is recommended that the documentation include the number of retries allowed, proofing alternatives (e.g., in-person if remote fails), or fraud countermeasures when anomalies are detected. Additional controls for handling identity proofing errors include:

- Advising the applicant of identity proofing failure and recourse options; and,
- Recording the errors in enrollment records/audit logs, along with any mitigating actions.

k. The CSP SHALL maintain a record, including audit logs, of all steps taken to verify the identity of the applicant as long as the identity exists in the information system.

SUPPLEMENTAL GUIDANCE: Ideally, the CSP's identity system includes the capability to securely record and log key security-related activities associated with the identity proofing process.

Examples of key steps that may be recorded in enrollment logs include:

- Identity information collected;
- Identity evidence provided;
- Identity evidence validated;
- Identity evidence validation source;
- Identity evidence binding verification method;
- Identity evidence verification result;
- Enrollment code confirmation result;
- enrollment result; and
- Authenticator enrollment binding

l. The CSP SHALL record the types of identity evidence presented in the proofing process.

SUPPLEMENTAL GUIDANCE: Ideally, the CSP's identity system includes the capability to securely record and log specific activities associated with the identity proofing process. For each piece of evidence collected or captured, the record should include:

1. Evidence type;
2. Determined strength;
3. Issuing source; and
4. Method of collection/capture*.

* Methods of collection and capture may include camera, flatbed scanner, bar code scanner.

m. The CSP SHALL conduct a risk management process, including assessments of privacy and security risks to determine:

1. Any steps that it will take to verify the identity of the applicant beyond any mandatory requirements specified herein;
2. The PII, including any biometrics, images, scans, or other copies of the identity evidence that the CSP will maintain as a record of identity proofing (Note: Specific federal requirements may apply); and
3. The schedule of retention for these records (Note: CSPs may be subject to specific retention policies in accordance with applicable laws, regulations, or policies, including any National Archives and Records Administration (NARA) records retention schedules that may apply).

SUPPLEMENTAL GUIDANCE: In accordance with its risk management processes, CSPs should conduct – and document the results of – privacy and security risk assessments. It is recommended that the scope of this assessment includes risks associated with:

- Any steps the CSP takes to verify applicant identities beyond what is required by the CJISSECPOL
- The CSP's collection, processing, and protection of PII, including any biometrics, images, scans, or other copies of the identity evidence that the CSP will maintain as a record of identity proofing;
- Retention and/or disposal of any records; and
- Adherence to any applicable federal requirements, laws, regulations or policies.

n. All PII collected as part of the enrollment process SHALL be protected to ensure confidentiality, integrity, and attribution of the information source.

SUPPLEMENTAL GUIDANCE: Unauthorized disclosure of PII can result in tangible and intangible harms to both the CSP as well as the subjects of the PII. After assessing the risks associated with collecting PII as part of its enrollment process, it is recommended that the CSP employ functional and technical mechanisms that adequately protect the confidentiality, integrity, and attribution of the PII under its control.

Such mechanisms may include:

- Limiting access to PII data;
- Privacy protecting policies;
- The use of encryption for data at rest and during transmission; and
- Integrity protection mechanisms such as hashes and record access logging.

o. "The entire proofing transaction, including transactions that involve a third party, SHALL occur over authenticated protected channels. "

SUPPLEMENTAL GUIDANCE: An encrypted communication channel uses approved cryptography where the connection initiator (client) has authenticated the recipient (server). Authenticated protected channels provide confidentiality and MitM attack protection and are frequently used in the user authentication process. Transport Layer Security* (TLS) is an example of an authenticated protected channel where the certificate presented by the recipient is verified by the initiator. Unless otherwise specified, authenticated protected channels do not require the server to authenticate the client.

Authentication of the server is often accomplished through a certificate chain leading to a trusted root rather than individually with each server.

*TLS version 1.2 or greater is recommended.

p. "If the CSP uses fraud mitigation measures, then the CSP SHALL conduct a privacy risk assessment for these mitigation measures. "

Such assessments SHALL include any privacy risk mitigations (e.g., risk acceptance or transfer, limited retention, use limitations, notice) or other technological mitigations (e.g., cryptography), and be documented per requirement IA-12(3) k – m above.

SUPPLEMENTAL GUIDANCE: This is a conditional requirement. CSPs may choose to obtain additional confidence in the identity proofing process beyond the requirements for IAL2 through additional fraud mitigation measures. Such measures may include:

- inspecting metadata information, such as by checking geolocation data associated with a mobile device used to send a photo or receive an SMS;
- examining the applicant’s device characteristics;
- evaluating behavioral characteristics, such as typing mannerisms, gait, or voice characteristics; and
- checking against authoritative sources, such as the Death Master File.

Employing one or more of these fraud mitigation techniques may result in the collection of additional PII about an applicant. Additional PII increases the potential impact of the unauthorized disclosure of this data. As part of the privacy risk assessment on these additional fraud mitigation measures, it is recommended that CSPs consider, at a minimum, the additional data (PII) that is processed, the implications of retaining this additional PII, and ways the associated risks can be minimized without negating the effects of the additional measures.

These additional fraud mitigation measures are not intended to substitute or replace the mandatory requirements. CSPs employing these measures are still responsible for meeting all applicable requirements.

q. In the event a CSP ceases to conduct identity proofing and enrollment processes, then the CSP SHALL be responsible for fully disposing of or destroying any sensitive data including PII, or its protection from unauthorized access for the duration of retention.

SUPPLEMENTAL GUIDANCE: This is a conditional requirement for CSPs that cease to perform identity proofing and enrollment functions. The CSP is responsible for the proper handling, protection, and retention or disposal of any sensitive data it collects, even after it ceases to provide identity proofing and enrollment services. A CSP may document its policies and procedures to the management of the data it collects in a data handling plan or other document. Additionally, it is recommended that CSPs document any specific retention policies they are subject to, in accordance with applicable laws, regulations, or policies, including any National Archives and Records Administration (NARA) records retention schedules that may apply.

Specifically, it is recommended that the CSP defines and documents the practices it has in place for fully disposing of or destroying any sensitive data including PII, or its continued protection from unauthorized access for the duration of any period of retention.

r. Regardless of whether the CSP is a federal agency or non-federal entity, the following requirements apply to the federal agency offering or using the proofing service:

1. The agency SHALL consult with their Senior Agency Official for Privacy (SAOP) to

- conduct an analysis determining whether the collection of PII to conduct identity proofing triggers Privacy Act requirements.
2. The agency SHALL publish a System of Records Notice (SORN) to cover such collection, as applicable.
 3. The agency SHALL consult with their SAOP to conduct an analysis determining whether the collection of PII to conduct identity proofing triggers E-Government Act of 2002 requirements.
 4. The agency SHALL publish a Privacy Impact Assessment (PIA) to cover such collection, as applicable.

SUPPLEMENTAL GUIDANCE: This requirement applies to Federal agencies whether providing authentication services directly or through a commercial provider. This requirement directs Agencies to consult with their Senior Agency Official for Privacy (SAOP) and conduct an analysis to determine whether the collection of PII to issue or maintain authenticators triggers the requirements of the Privacy Act of 1974 or the requirements of the E-Government Act of 2002. Based on this consultation and analysis, the agency may need to publish a System of Records Notice (SORN) and/or a Privacy Impact Assessment (PIA) to cover such collections, as applicable. While this requirement specifically applies only to federal agencies, CSPs that provide services to federal agencies may be expected to provide information about their identity services in support of an Agency's privacy analysis and PIA.

- s. An enrollment code SHALL be comprised of one of the following:
 - 1 Minimally, a random six character alphanumeric or equivalent entropy. For example, a code generated using an approved random number generator or a serial number for a physical hardware authenticator; OR
 - 2 A machine-readable optical label, such as a QR Code, that contains data of similar or higher entropy as a random six character alphanumeric.

SUPPLEMENTAL GUIDANCE: The use of an enrollment code for address confirmation is a requirement for IAL2 remote identity proofing and enrollment. CSPs that perform in-person identity at IAL2 may voluntarily choose to use enrollment codes for such binding, but this is not required. Enrollment codes may also be used for in-person proofing and enrollment processes if an authenticator(s) is not registered to the subscribers' account at the time of in-person identity proofing and, therefore, the authenticator binding would need to occur at a later time. Enrollment codes may be used for authenticator binding to subscribers' accounts in such circumstances.

Enrollment code use for IAL2 remote identity proofing allows the CSP to confirm that the applicant controls a validated address of record. Authenticator binding may not be completed in the same session for in-person identity proofing. Enrollment codes may be used for binding an authenticator to subscribers' accounts at a later time in such circumstances. The requirements presented in this criterion apply to all enrollment codes that may be used by the CSP for any purpose.

Enrollment code use has the additional requirement for code validity periods. The validity period is determined by the type of address where the enrollment code is sent, as follows:

- 10 days, when sent to a postal address of record within the contiguous United States;
- 30 days, when sent to a postal address of record outside the contiguous United States;

- 10 minutes, when sent to a telephone of record (SMS or voice);
- 24 hours, when sent to an email address of record;
- 7 days if provided directly to the applicant during an in-person proofing session for authenticator binding at IAL2.

These validity periods are presented again in requirement IA-12 (5) g which presents the mandatory requirement for enrollment code confirmation for IAL2 remote identity proofing.

t. Training requirements for personnel validating evidence SHALL be based on the policies, guidelines, or requirements of the CSP or RP.

SUPPLEMENTAL GUIDANCE: The training requirement pertains to personnel performing the validation of identity evidence but does not specify training content. The CSP policies, guidelines, or requirements for validating identity evidence for identity proofing would be appropriate for the type of training intended by this requirement. Such content may include:

- the CSP's policy for types of evidence it collects and validates in order to meet the requirements of designated IALs;
- validation of security features for the types of identity evidence collected;
- detection of evidence alteration, falsification, or forgery for the types of identity evidence collected. Procedures for the validation of identity evidence information with issuing and authoritative sources.

This training may be accomplished through written training material, oral instruction, on-the-job training and mentoring, or other means. CSPs may perform some of the requirements for identity evidence validation through automated services and equipment. Therefore, personnel training would be based on the CSPs policies and procedures for the manual performance of evidence validation.

u. This criterion applies to CSPs that provide identity proofing and enrollment services to minors (under the age of 18):

If the CSP provides identity proofing and enrollment services to minors (under the age of 18), then...the CSP SHALL give special consideration to the legal restrictions of interacting with minors unable to meet the evidence requirements of identity proofing [to ensure compliance with the Children's Online Privacy Protection Act of 1998 (COPPA), and other laws, as applicable]. "

SUPPLEMENTAL GUIDANCE: In general, minors will not possess the types of evidence required to meet the CSP's minimum requirements for a given IAL. ICSPs that provide identity services to minors will need to determine and document the special considerations it applies to minors. Such special considerations may include the use of trusted referees and an expanded list of acceptable evidence types to include evidence a minor would likely possess, such as school IDs.

Requirements 'v' and 'w' apply to the collection of biometric characteristics for in-person (physical or supervised remote) identity proofing and are mandatory at IAL3. These criteria also

apply to CSPs that optionally choose to collect biometric characteristics through in-person identity proofing and enrollment at IAL2.

v. The CSP SHALL have the operator view the biometric source (e.g., fingers, face) for presence of non-natural materials and perform such inspections as part of the proofing process.

SUPPLEMENTAL GUIDANCE: Applicants may try to defraud the identity proofing process by using fake fingers or by applying non-natural materials - such as latex, silicon, or glue – to their fingers, faces, or other sources of biometrics. It is recommended that identity proofing operators be trained to recognize such practices and to examine all biometric sources used in the identity proofing for the presence of foreign materials.

It is recommended that the CSP documents and applies technologies and procedures which ensure that the proofing operator reviews the biometric source (e.g., fingers, face) for presence of non-natural materials and perform such inspections as part of the proofing process.

Requirements ‘v’ and ‘w’ apply to the collection of biometric characteristics for in-person (physical or supervised remote) identity proofing and are mandatory at IAL3. These criteria also apply to CSPs that collect biometric characteristics through in-person identity-proofing identity proofing and enrollment at IAL2.

w. The CSP SHALL collect biometrics in such a way that ensures that the biometric is collected from the applicant, and not another subject. All biometric performance requirements in IA-5 m (1) through (12) apply.

SUPPLEMENTAL GUIDANCE: Applicants may try to defraud the identity proofing process by having another person present themselves for biometric collection. The risk of this happening is increased if the identity proofing process is not completed in a single session and during supervised remote identity proofing processes.

Documenting the technologies and procedures the CSP employs to ensure that biometric samples are taken from the applicant him/herself and not another person facilitates the assessment against this requirement.

x. The CSP SHALL support in-person or remote identity proofing, or both.

SUPPLEMENTAL GUIDANCE: IAL2 allows for remote or in-person identity proofing. IAL2 supports a wide range of acceptable identity proofing techniques in order to increase user adoption, decrease false negatives (legitimate applicants that cannot successfully complete identity proofing), and detect to the best extent possible the presentation of fraudulent identities by a malicious applicant.

Remote proofing presents challenges to achieving the desired outcomes described above that can be overcome through the use specific processes and technologies. Potential processes and controls that CSPs may employ to mitigate risks associated with remote identity proofing at IAL2 include:

1. A remote operator is present during at least part of the identity proofing session and

can provide positive confirmation that the requirements for IAL2 identity proofing are met. Employing real-time remote operators provides the capability for the identity proofing process to be completed in a single session and allows the remote operator to direct the applicant for proper presentation and examination of identity evidence and biometrics collection.

2. The CSP employs automated technologies and services (e.g., liveness detection, identity evidence verification and validation, and presentation attack detection, if applicable) which can ensure the requirements for IAL2 identity proofing are met and protect against spoofing attacks. This process also provides the capability for the identity proofing process to be completed in a single session.
 3. The CSP employs an off-line operator to evaluate the evidence and images collected during a previous identity proofing process. In this scenario, the identity proofing process requires more than one session with the applicant and is not completed until the operator provides a positive confirmation that all requirements for IAL2 identity proofing are met.
- y. The CSP SHALL collect the following from the applicant:
1. One piece of SUPERIOR or STRONG evidence if the evidence's issuing source, during its identity proofing event, confirmed the claimed identity by collecting two or more forms of SUPERIOR or STRONG evidence and the CSP validates the evidence directly with the issuing source; OR
 2. Two pieces of STRONG evidence; OR
 3. One piece of STRONG evidence plus two pieces of FAIR evidence

SUPPLEMENTAL GUIDANCE: The goal of identity validation is to collect the most appropriate identity evidence (e.g., a passport or driver's license) from the applicant and determine its authenticity, validity, and accuracy. Identity validation is made up of three process steps: 1) collecting the appropriate identity evidence, 2) confirming the evidence is genuine and authentic, and 3) confirming the data contained on the identity evidence is valid, current, and related to a real-life subject.

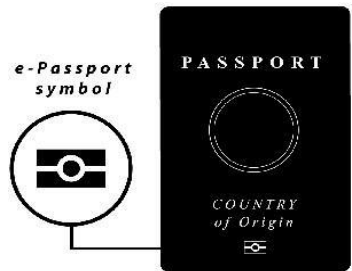
Figure 9 - Notional Strength of Evidence Types of this document presents notional strengths for types of evidence that may be presented for identity proofing purposes. Documenting the types and strengths of evidence the CSP collects for each proofing encounter demonstrates conformance for this requirement. (Also see IA-12 (3) 1.)

Examples of methods and how they can be used to capture identity evidence images or extract data for validation include:

- Cameras to capture images of identity evidence for the purposes of evidence validation;
- Document scanner to capture images of identity evidence for the purpose of evidence validation; and
- Bar-code scanner to capture and extract information from standardized barcodes embedded on identity evidence.

High resolution images of at least 300 ppi are necessary for proper evidence examination and validation.

Figure 7 – Notional Strengths of Evidence Types

Type of Evidence	Strength	Notes
US Passport	Superior	Includes US Passport cards
Foreign e-Passport	Superior	 <p>The diagram illustrates a foreign e-Passport. On the left is a circular 'e-Passport symbol' containing a stylized 'E' with a circle in the center. A line connects this symbol to a rectangular passport cover on the right. The cover is dark with 'PASSPORT' at the top, a circular emblem in the center, and 'COUNTRY of Origin' at the bottom.</p>
Personal Identity Verification (PIV) card	Superior	
Common Access card (CAC)	Superior	
Personal Identity Verification Interoperable (PIV-I) card	Superior	
Transportation Worker Identification Credential (TWIC)	Superior	
Permanent Resident Card	Superior	Issued on or after May 11, 2010
Native American Enhanced Tribal Card	Superior	

Type of Evidence	Strength	Notes
REAL ID cards	Strong+	Includes REAL ID driver's licenses and ID cards. REAL ID cards have a star printed in the upper right-hand corner. Card and personal information must be validated with appropriate DMV or AAMVA.
Enhanced ID cards	Strong+	Includes Enhanced ID driver's licenses and ID cards. Must be validated with appropriate DMV or AAMVA.
U.S. Uniformed Services Privilege and Identification Card (U.S. Military ID)	Strong+	Includes Uniformed Services Dependent ID Cards. Must be validated with appropriate military issuing source.
Permanent Resident Card	Strong	Issued Prior to May 11, 2010
Native American Tribal Photo Identification Card	Strong	
Driver's License or ID card (REAL ID non-compliant)	Strong	
School ID card	Fair	Includes facial image photograph
Utility account statement	Fair	
Credit/debit card and account statement	Fair	
Financial institution account statement	Fair	

Type of Evidence	Strength	Notes
US Social Security Card	Weak	
Original or certified copy of a birth certificate issued by a state, county, municipal authority or outlying possession of the United States bearing an official seal	Weak	

z. The CSP SHALL validate each piece of evidence with a process that can achieve the same strength as the evidence presented (see ‘y’ above). For example, if two forms of STRONG identity evidence are presented, each piece of evidence will be validated at a strength of STRONG.

SUPPLEMENTAL GUIDANCE: The goal of identity validation is to collect the most appropriate identity evidence (e.g., a passport, driver’s license) from the applicant and determine its authenticity, validity, and accuracy. Identity validation is made up of three process steps: 1) collect the appropriate identity evidence, 2) confirm the evidence is genuine and authentic, and 3) confirm the data contained on the identity evidence is valid, current, and related to a real-life subject.

Evidence validation for authenticity involves examining the evidence for:

- Confirmation of required information completeness and format for the identity evidence type.
- Detection of evidence tampering or the creation of counterfeit or fraudulent evidence.
- Confirmation of security features. See Figure 10 - Types of Identity Evidence Security Features to this document for types of commonly used security features for identity evidence.

Most of the capabilities to confirm security features on identity evidence are dependent upon physically viewing the evidence directly, tactile feel of the evidence, and viewing the evidence under specialized lighting or through the use of specialized equipment (see Figure 10 - Types of Identity Evidence Security Features). Therefore, the validation of evidence that may be submitted remotely for remote identity proofing methods is particularly challenging. For this reason, CSPs opting to provide remote identity proofing may find it most effective to use automated evidence validation products and services. If automated evidence validation solutions are not used, CSPs may choose to apply similar procedures for IAL2 remote proofing as are required for IAL3 supervised remote proofing. These procedures provide that a trained operator can remotely supervise the evidence collection process, require the applicant to turn or tilt evidence or apply lighting to be able to confirm security features on evidence that is presented for the identity proofing encounter in a recorded video or webcast. Alternatively, a CSP may use an automated interface for the capture

of identity evidence images that similarly can direct the applicant to turn, tilt or provide lighting on evidence presented for identity proofing purposes.

Figure 8 – Types of Identity Evidence Security Features

Security Feature (examination capability)	Description
Fine-line or Guilloche Pattern (visual)	Background pattern of continuous fine lines printed in wavy, overlapping pattern.
Ghost image (visual)	Half-tone reproduction of original image (e.g., facial image), may be printed behind printed data.
Overlapped data (visual)	Variable data (e.g., signature, seal, text) printed over another field such as facial image or seal.
Transparent image (visual)	See-through, window-like image feature (e.g., facial image) visible for both sides of the evidence.
Rainbow printing (visual)	Controlled color shifts of printed text in a continuous, linear fashion.
Holographic Images (visual, tilting)	Light field record of objects that will appear and change as view of evidence is tilted and turned. Most state-issued driver's licenses and IDs contain at least one holographic image.
Variable laser engraved images (visual, tilting)	Laser-engraved images at different angles so that image view changes with tilting angle of viewing evidence.
Iridescent Inks and Custom Foil Stamping (visual, tilting)	Custom designs and printing that will change color properties depending on the angle at which evidence is viewed.
Laser perforation (visual, light, tactile)	Perforated holes made by laser beam to form images. The images can be viewed under light source; image holes have tactile feel.
UV printing (visual, UV lighting)	A UV image or text that can only be viewed with special lighting. UV images may appear on the front or back of the evidence.

Security Feature (examination capability)	Description
Microprinting (visual, magnifier)	Microtext of static or variable data that can be confirmed when viewed under a magnifier. Requires magnification of at least 10X to view.
Laser embossing (tactile)	Use of laser to emboss image or text for tactile feel on only one side of the evidence.
Barcode (visual, barcode reader)	Machine readable, encoded data (typically personalized printed data) for 2-D barcode, readable with barcode reader.
UV printing (visual, UV lighting)	A UV image or text that can only be viewed with specialized lighting. UV images may appear on the front or back of a card.

The next step in identity evidence validation for authenticity and integrity is to verify the correctness of information from the identity evidence against the issuing source for the evidence or an authoritative source that has linkage to the issuing source. Results of these checks for authenticity and integrity should be recorded.

Figure 11 - Validating Identity Evidence lists strengths, ranging from unacceptable to superior, of identity validation performed by the CSP to validate the evidence presented for the current proofing session and the information contained therein.

Figure 9 – Validating Identity Evidence

Strength	Method(s) Performed by the CSP
Unacceptable	<ul style="list-style-type: none"> Evidence validation was not performed, or validation of the evidence failed.
Weak	<ul style="list-style-type: none"> All personal details from the evidence have been confirmed as valid by comparison with information held or published by an authoritative source.

Strength	Method(s) Performed by the CSP
Fair	<ul style="list-style-type: none"> Attributes contained in the evidence have been confirmed as valid by comparison with information held or published by the issuing source or authoritative source(s), OR The evidence has been confirmed as genuine using appropriate technologies, confirming the integrity of physical security features and that the evidence is not fraudulent or inappropriately modified, OR The evidence has been confirmed as genuine by trained personnel, OR The evidence has been confirmed as genuine by confirmation of the integrity of cryptographic security features.
Strong	<ul style="list-style-type: none"> The evidence has been confirmed as genuine: <ul style="list-style-type: none"> using appropriate technologies, confirming the integrity of physical security features and that the evidence is not fraudulent or inappropriately modified, OR by trained personnel and appropriate technologies, confirming the integrity of the physical security features and that the evidence is not fraudulent or inappropriately modified, OR by confirmation of the integrity of cryptographic security features. All personal details and evidence details have been confirmed as valid by comparison with information held or published by the issuing source or authoritative source(s).
Superior	<ul style="list-style-type: none"> The evidence has been confirmed as genuine by trained personnel and appropriate technologies including the integrity of any physical and cryptographic security features. All personal details and evidence details from the evidence have been confirmed as valid by comparison with information held or published by the issuing source or authoritative source(s).

aa. The CSP SHALL verify identity evidence as follows:

At a minimum, the applicant's binding to identity evidence must be verified by a process that is able to achieve a strength of STRONG.

SUPPLEMENTAL GUIDANCE: The goal of identity verification is to confirm and establish a linkage between the validated evidence for the claimed identity and the real-life applicant presenting the evidence

The figure below shows IAL2 verification methods.

Figure 10 – Verification Methods and Strengths

Verification Strength	Verification Method	Description
Superior	Biometric Verification	Biometric comparison against biometric characteristics on the strongest piece(s) of evidence against live biometric capture for remote or in-person identity proofing. May be used for identity verification for FAIR, STRONG, and SUPERIOR strength.
Strong	In-Person Physical Verification	Physical comparison of applicant to facial-image photograph on strongest piece(s) of validated evidence. May be used for identity verification for FAIR and STRONG strength.
Strong	Remote Physical Verification	Physical comparison of applicant to facial-image photograph on strongest piece(s) of validated evidence. May be used for identity verification for FAIR and STRONG strength.

For IAL2 this linkage is achieved through a physical or biometric comparison of the facial image (i.e., photograph) on the strongest piece of evidence to the applicant or by a biometric comparison between information on the evidence and a biometric characteristic obtained from the applicant, most likely facial image.

Physical comparison is a comparison by a person (i.e., CSP-trained personnel) of the applicant to the photograph (i.e., facial image) on any of the strongest piece(s) of validated identity evidence collected. This comparison can be an in-person comparison for in-person identity proofing processes or may be conducted remotely for remote identity proofing. In both cases, the operator must perform a physical comparison of the applicant to the facial image photograph on the evidence. That is, the in-person proofing personnel will physically compare the facial image of the live applicant to the facial image photograph on the strongest piece of validated evidence. For remote physical comparison, the applicants' facial image may be captured by high resolution video or camera for physical comparison to the facial image photograph on the identity evidence.

For identity proofing verification, biometric comparison is an automated comparison of a biometric characteristic recorded on the strongest piece of identity evidence compared to the corresponding biometric characteristic of the applicant captured live during the identity proofing session.

Remote identity proofing requires the collection of both an image of the identity evidence and a live capture of the facial image of the applicant for physical or biometric comparison. The CSP must employ liveness and presentation attack detection capabilities to ensure that the applicant's facial image or other biometric characteristic used for comparison is "live" and not a spoofing or

presentation attack. Potential methods for remote identity proofing processes to mitigate such spoofing and presentation attacks are presented below.

- A remote operator is present during the identity proofing session (similar to supervised remote in-person proofing) and can conduct a real-time physical comparison between an image of the identity evidence and a live video of the applicant. In order to confirm the video stream is live and not pre-recorded, the Operator could direct the applicant to move their head in specific ways, or even ask the applicant a question. Once a positive confirmation is recorded from the operator, and all other requirements are met, the identity proofing can be completed in a single session.
- The CSP employs automated capabilities which are specifically designed to compare the image of the identity evidence with the applicant, and which also employ liveness detection technologies. Pending a positive confirmation from the automated comparison, and the satisfaction of all other requirements, the identity proofing can be completed in a single session.

The CSP employs liveness detection technology during the capture of the facial image, and an off-line operator performs the physical comparison of images captured during the identity proofing session. The identity proofing process requires more than one session with the applicant and is not completed until the operator provides a positive confirmation of the comparison and the other requirements are met.

bb. For IAL2 remote proofing: The collection of biometric characteristics for physical or biometric comparison of the applicant to the strongest piece of identity evidence provided to support the claimed identity performed remotely SHALL adhere to all requirements as specified in IA-5 m.

SUPPLEMENTAL GUIDANCE: See IA-5 m (1) – (12) for conformance criteria for the implementation and conformance assessment of requirements for the use of biometrics.

cc. Knowledge-based verification (KBV) SHALL NOT be used for in-person (physical or supervised remote) identity verification.

SUPPLEMENTAL GUIDANCE: identity verification is performed against the strongest piece of identity evidence submitted and validated. For IAL2 the strongest piece of evidence will always be either STRONG or SUPERIOR evidence. KBV (sometimes referred to as knowledge-based authentication) is only permitted as a verification method for evidence at the FAIR strength level; therefore, verification of FAIR evidence binding will never be required for IAL2.

dd. The CSP SHALL employ appropriately tailored security controls, to include control enhancements, from the moderate or high baseline of security controls defined in the CJISSECPOL.

The CSP SHALL ensure that the minimum assurance-related controls for moderate-impact systems are satisfied.

ee. Supervised Remote Identity Proofing: Supervised remote identity proofing is intended to provide controls for comparable levels of confidence and security to in-person IAL3 identity proofing for identity proofing processes that are performed remotely. Supervised remote identity proofing is optional for CSPs; that is, if a CSP chooses to use supervised remote identity proofing, then the following requirements, (1) through (8), would apply. It should be noted that the term “supervised remote identity proofing” has specialized meaning and is used only to refer to the specialized equipment and the following control requirements, (1) through (8). In addition to those requirements presented in this document, as well as the applicable identity validation and verification requirements, CSPs that provide supervised remote identity proofing services must demonstrate conformance with the requirements contained in this section. The following requirements for supervised remote proofing apply specifically to IAL3. If the equipment/facilities used for supervised remote proofing are used for IAL2 identity proofing, the following requirements, (1) through (8), for supervised remote proofing do not apply. In this case, the requirements for conventional remote identity proofing are applicable.

1. Supervised remote identity proofing and enrollment transactions SHALL meet the following requirements, in addition to the IAL3 validation and verification requirements specified in IA-12(3)s.

SUPPLEMENTAL GUIDANCE: Supervised remote identity proofing involves the use of a CSP-controlled station at a remote location that is connected to a trained operator at a central location. The goal of this arrangement is to permit identity proofing of individuals in remote locations where it is not practical for them to travel to the CSP for in-person identity proofing.

2. The CSP SHALL monitor the entire identity proofing session, from which the applicant SHALL NOT depart — for example, by a continuous high-resolution video transmission of the applicant.

SUPPLEMENTAL GUIDANCE: The integrity of supervised remote identity proofing depends upon the applicant being continuously present during the entire session. An applicant who steps away from an in-process session may do so to alter their biometric source or substitute a different person to complete the identity proofing process.

3. The CSP SHALL have a live operator participate remotely with the applicant for the entirety of the identity proofing session.

SUPPLEMENTAL GUIDANCE: Having a trained operator supervise and participate in a remote identity proofing session reduces the opportunity for an applicant to defraud the process. As described in Appendix A Terms and Definitions, the operator is a person who has received specific training on enrollment and identity proofing procedures and the detection of potential fraud by an applicant.

4. The CSP SHALL require all actions taken by the applicant during the identity proofing session to be clearly visible to the remote operator.

SUPPLEMENTAL GUIDANCE: The camera(s) a CSP employs to monitor the actions taken by a remote applicant during the identity proofing session should be positioned in such a way that the upper body, hands, and face of the applicant are always visible. Additionally, the components of the remote identity proofing station (including such things as keyboard, fingerprint capture device, signature pad, and scanner, as applicable) should be arranged such that all interactions with these devices is within the field of view.

5. The CSP SHALL require that all digital validation of evidence (e.g., via chip or wireless technologies) be performed by integrated scanners and sensors.

SUPPLEMENTAL GUIDANCE: Technologies exist that allow for the digital validation of identity evidence via electronic means (such as RFID to read the data off e-passports and chip readers for smartcards). The scanners and sensors employed to access these features should be integrated into the remote identity proofing stations in order to reduce the likelihood of being tampered with, removed, or replaced. To be integrated means the devices themselves are a component of the workstation (i.e., smartcard readers or fingerprint sensors built into a laptop) or the devices, and their connections, are secured in a protective case or locked box.

6. The CSP SHALL require operators to have undergone a training program to detect potential fraud and to properly perform a supervised remote proofing session.

SUPPLEMENTAL GUIDANCE: A comprehensive training program for supervised remote identity proofing operators may include some or all the following:

- Purpose and objectives of the identity proofing and enrollment process, as employed by the CSP;
- Supervised remote identity proofing process workflow;
- Identity evidence validation processes;
- Threats associated with the identity proofing process and how to detect potential fraud; and
- System and process troubleshooting and problem resolution.

7. The CSP SHALL employ physical tamper detection and resistance features appropriate for the environment in which it is located.

SUPPLEMENTAL GUIDANCE: For example, a kiosk located in a restricted area or one where it is monitored by a trusted individual requires less tamper detection than one that is located in a semi-public area such as a shopping mall concourse.

8. The CSP SHALL ensure that all communications occur over a mutually authenticated protected channel.

SUPPLEMENTAL GUIDANCE: Mutually authenticated protected channels employ approved cryptography to encrypt communications between

- ff. Trusted Referee: The use of trusted referees is optional for CSPs; that is, if a CSP chooses to use trusted referees for identity proofing and enrollment, then the following requirements, (1) through (3), would apply. The use of trusted referees is intended to assist in the identity proofing and enrollment for populations that are unable to meet IAL2 identity proofing requirements, or otherwise would be challenged to perform identity proofing and enrollment process requirements. Such populations may include, but are not limited to:

- disabled individuals;
- elderly individuals;
- homeless individuals,
- individuals with little or no access to online services or computing devices;
- unbanked and individuals with little or no credit history;
- victims of identity theft;
- children under 18; and
- immigrants.

In addition to those requirements presented in the General section of this document, as well as the applicable IAL requirements, CSPs that use trusted referees in their identity proofing services must demonstrate conformance with the requirements contained in this section.

1. If the CSP uses trusted referees, then...The CSP SHALL establish written policy and procedures as to how a trusted referee is determined and the lifecycle by which the trusted referee retains their status as a valid referee, to include any restrictions, as well as any revocation and suspension requirements.

SUPPLEMENTAL GUIDANCE: In instances where an individual cannot meet the identity evidence requirements specified in IA-12 (3) y – ee and IA-12 (5) b - i, the agency may use a trusted referee to assist in identity proofing the applicant. It is intended that CSPs using trusted referees for identity proofing and enrollment will document the procedures and controls in an applicable written policy or *practice statement* as described in IA-12 (3) h.

2. If the CSP uses trusted referees, then...The CSP SHALL proof the trusted referee at the same IAL as the applicant proofing.

SUPPLEMENTAL GUIDANCE: Trusted referees, who participate in the identity proofing process on behalf of an applicant need to be identity proofed themselves to the same level as that of the applicant. If CSPs allow the use of Trusted Referees, its documented policies should state this requirement.

3. If the CSP uses trusted referees, then...The CSP SHALL determine the minimum evidence required to bind the relationship between the trusted referee and the applicant.

SUPPLEMENTAL GUIDANCE: In addition to proofing a Trusted Referee to the same (or greater) IAL as that of the applicant, CSPs will need to determine its process for proving a legitimate relationship to the applicant. The CSP should consider and document the types of evidence (i.e., power of attorney) it will accept to “bind” the relationship between Trusted Referee and an applicant. This minimum evidence may vary based on IAL.

Related Controls: None.

(5) IDENTITY PROOFING | ADDRESS CONFIRMATION

[Priority 2]

Control:

- a. Require that a registration code or notice of proofing be delivered through an out-of-band channel to verify the user's address (physical or digital) of record.

DISCUSSION: To make it more difficult for adversaries to pose as legitimate users during the identity proofing process, organizations can use out-of-band methods to ensure that the individual associated with an address of record is the same individual that participated in the registration. Confirmation can take the form of a temporary enrollment code or a notice of proofing. The delivery address for these artifacts is obtained from records and not self-asserted by the user. The address can include a physical or digital address. A home address is an example of a physical address. Email addresses and telephone numbers are examples of digital addresses.

- b. The CSP SHALL confirm address of record.

SUPPLEMENTAL GUIDANCE: Valid records to confirm address are issuing source(s) or authoritative source(s). Ideally, the CSP will confirm an address of record through validation of the address contained on any supplied, valid piece of identity evidence. However, the CSP may confirm address of record by validating information supplied by the applicant that is not contained on any supplied piece of identity evidence. Postal addresses are preferred, however these guidelines support any type of address that can be validated against an issuing or authoritative source, whether physical or digital. Acceptable addresses of record include postal addresses, email addresses, and telephone numbers. The types of addresses of record a CSP accepts will determine, in part, the method it employs to validate them. For instance, postal addresses can be validated by confirming it against a piece of supplied, valid identity evidence. Email addresses may be confirmed by sending an email to the provided address.

- c. Valid records to confirm address SHALL be issuing source(s) or authoritative source(s).

Self-asserted address data that has not been confirmed in records SHALL NOT be used for confirmation.

SUPPLEMENTAL GUIDANCE: An address of record is a “validated and verified location (physical or digital) where an individual can receive communications using approved mechanisms.” IAL2 requires confirming an applicant’s address of record. This can be accomplished in two ways: 1) validation of the address contained on a valid piece of identity evidence, or 2) by employing a mechanism such as enrollment codes to validate an address not contained on a supplied piece of identity evidence.

Addresses that are supplied by an applicant, either verbally or on a non-valid piece of identity evidence, are not valid for confirming an applicant’s address of record.

- d. Note that IAL2-7 applies only to in-person proofing at IAL2.

If the CSP performs in-person proofing for IAL2 and provides an enrollment code directly to the subscriber for binding to an authenticator at a later time, then the enrollment code...SHALL be valid for a maximum of seven (7) days.

SUPPLEMENTAL GUIDANCE: Upon successful completion of the identity proofing process the CSP will typically register one or more authenticators to the subscribers’ account or may optionally choose to bind an authenticator(s) at a later time. If the CSP chooses to use an enrollment code provided directly to the applicant to authenticate for such later binding, the validity period for the enrollment code is a maximum of seven days (see IA-12 (3) s).

Note that conformance criteria IA-12 (5) ‘e’ through ‘i’ apply to remote identity proofing processes at IAL2.

- e. For remote identity proofing at IAL2:

The CSP SHALL send an enrollment code to a confirmed address of record for the applicant.

SUPPLEMENTAL GUIDANCE: Enrollment codes used for IAL2 remote identity proofing may be sent to any confirmed address of record – postal, mobile phone number for SMS, or email addresses.

- f. For remote identity proofing at IAL2:

The applicant SHALL present a valid enrollment code to complete the identity proofing process.

SUPPLEMENTAL GUIDANCE: Per IA-12 (5) e above, sending an enrollment code to a confirmed address of record, as captured during the identity proofing process, is required to complete the remote identity proofing process and provides additional confidence in the binding of that address to the applicant.

Valid enrollment codes mean that the correct enrollment code is submitted by the applicant within prescribed validity periods. Enrollment code validity periods depend on the type of address where the code is sent as shown in IA-12 (5) g below.

Information captured in the CSP's enrollment records or system logs facilitate assessment against this requirement. Ideally, this information would include details about the validity of the enrollment code (date and time applicant entered code; confirmation it was the correct code; and confirmation it was not expired).

- g. Note that the following enrollment code validity periods apply to enrollment codes sent to confirmed addresses of record for IAL2 remote in-person proofing only.

Enrollment codes shall have the following maximum validities:

1. 10 days, when sent to a postal address of record within the contiguous United States;
2. 30 days, when sent to a postal address of record outside the contiguous United States;
3. 10 minutes, when sent to a telephone of record (SMS or voice);
4. 24 hours, when sent to an email address of record.

SUPPLEMENTAL GUIDANCE: Enrollment codes sent to addresses of record are only valid for a limited amount of time, depending on the type of address of record to which they are sent. Applicants that present enrollment codes that are no longer valid (aka, expired) cannot use this code to complete their identity proofing process.

- h. If the enrollment code sent to the confirmed address of record as part of the remote identity proofing process at IAL2 is also intended to be an authentication factor, then...it SHALL be reset upon first use.

SUPPLEMENTAL GUIDANCE: Enrollment codes sent as an authentication factor for address confirmation may only be used once.

- i. If the CSP performs remote proofing at IAL2 and optionally sends notification of proofing in addition to sending the required enrollment code, then...The CSP SHALL ensure the enrollment code and notification of proofing are sent to different addresses of record.

SUPPLEMENTAL GUIDANCE: For example, if the CSP sends an enrollment code to a phone number validated in records, a proofing notification may be sent to the postal address validated in records or obtained from validated and verified evidence, such as a driver's license.

Related Controls: IA-12.

INCIDENT RESPONSE (IR)

IR-1 POLICY AND PROCEDURES

[Existing] [Priority 2]

Control:

- a. Develop, document, and disseminate to all personnel when their unescorted logical or physical access to any information system results in the ability, right, or privilege to view, modify, or make use of unencrypted CJI:
 1. Agency-level incident response policy that:
 - a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 - b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
 2. Procedures to facilitate the implementation of the incident response policy and the associated incident response controls;
- b. Designate an individual with security responsibilities to manage the development, documentation, and dissemination of the incident response policy and procedures; and
- c. Review and update the current incident response:
 1. Policy annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI; and
 2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.

Discussion: Incident response policy and procedures address the controls in the IR family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of incident response policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to incident response policy and procedures include assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PS-8, SI-12.

IR-2 INCIDENT RESPONSE TRAINING

[Existing] [Priority 2]

Control:

- a. Provide incident response training to system users consistent with assigned roles and responsibilities:
 1. Prior to assuming an incident response role or responsibility or acquiring system access;
 2. When required by system changes; and
 3. Annually thereafter; and
- b. Review and update incident response training content annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.

Discussion: Incident response training is associated with the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail are included in such training. For example, users may only need to know who to call or how to recognize an incident; system administrators may require additional training on how to handle incidents; and incident responders may receive more specific training on forensics, data collection techniques, reporting, system recovery, and system restoration. Incident response training includes user training in identifying and reporting suspicious activities from external and internal sources. Incident response training for users may be provided as part of AT-2 or AT-3.

Events that may precipitate an update to incident response training content include, but are not limited to, incident response plan testing or response to an actual incident (lessons learned), assessment or audit findings, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Related Controls: AT-2, AT-3, AT-4, CP-3, IR-3, IR-4, IR-8.

Control Enhancements:

(3) INCIDENT RESPONSE TRAINING | BREACH

[Priority 3]

Control:

Provide incident response training on how to identify and respond to a breach, including the organization's process for reporting a breach.

Discussion: For federal agencies, an incident that involves personally identifiable information is considered a breach. A breach results in the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or a similar occurrence where a person other than an authorized user accesses or potentially accesses personally identifiable information or an authorized user accesses or potentially accesses such information for other than authorized purposes. The incident response training emphasizes the obligation of individuals to report both confirmed and suspected breaches involving information in any medium or form, including paper, oral, and electronic. Incident response training includes tabletop exercises that simulate a breach.

IR-3 INCIDENT RESPONSE TESTING

[Priority 3]

Control:

Test the effectiveness of the incident response capability for the system annually using the following tests: tabletop or walk-through exercises; simulations; or other agency-appropriate tests.

Discussion: Organizations test incident response capabilities to determine their effectiveness and identify potential weaknesses or deficiencies. Incident response testing includes the use of checklists, walk-through or tabletop exercises, and simulations (parallel or full interrupt). Incident response testing can include a determination of the effects on organizational operations and assets and individuals due to incident response. The use of qualitative and quantitative data aids in determining the effectiveness of incident response processes.

Related Controls: CP-3, CP-4, IR-2, IR-4, IR-8.

Control Enhancements:

(2) INCIDENT RESPONSE TESTING | COORDINATION WITH RELATED PLANS

[Priority 3]

Control:

Coordinate incident response testing with organizational elements responsible for related plans.

Discussion: Organizational plans related to incident response testing include business continuity plans, disaster recovery plans, continuity of operations plans, contingency plans, crisis communications plans, critical infrastructure plans, and occupant emergency plans.

IR-4 INCIDENT HANDLING

[Existing] [Priority 2]

Control:

- a. Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery;
- b. Coordinate incident handling activities with contingency planning activities;
- c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly; and
- d. Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.

Discussion: Organizations recognize that incident response capabilities are dependent on the capabilities of organizational systems and the mission and business processes being supported by those systems. Organizations consider incident response as part of the definition, design, and

development of mission and business processes and systems. Incident-related information can be obtained from a variety of sources, including audit monitoring, physical access monitoring, and network monitoring; user or administrator reports; and reported supply chain events. An effective incident handling capability includes coordination among many organizational entities (e.g., mission or business owners, system owners, authorizing officials, human resources offices, physical security offices, personnel security offices, legal departments, risk executive [function], operations personnel, procurement offices). Suspected security incidents include the receipt of suspicious email communications that can contain malicious code. Suspected supply chain incidents include the insertion of counterfeit hardware or malicious code into organizational systems or system components. For federal agencies, an incident that involves personally identifiable information is considered a breach. A breach results in unauthorized disclosure, the loss of control, unauthorized acquisition, compromise, or a similar occurrence where a person other than an authorized user accesses or potentially accesses personally identifiable information or an authorized user accesses or potentially accesses such information for other than authorized purposes.

Related Controls: AC-19, AU-6, AU-7, CM-6, CP-2, CP-3, CP-4, IR-2, IR-3, IR-5, IR-6, IR-8, PE-6, PL-2, SA-8, SC-5, SC-7, SI-3, SI-4, SI-7.

Control Enhancements:

(1) INCIDENT HANDLING | AUTOMATED INCIDENT HANDLING PROCESSES

[Existing] [Priority 2]

Control:

Support the incident handling process using automated mechanisms (e.g., online incident management systems and tools that support the collection of live response data, full network packet capture, and forensic analysis).

Discussion: Automated mechanisms that support incident handling processes include online incident management systems and tools that support the collection of live response data, full network packet capture, and forensic analysis. Incident handling could be inherited from an upstream agency or could be part of a state-level process.

IR-5 INCIDENT MONITORING

[Existing] [Priority 2]

Control: Track and document incidents.

Discussion: Documenting incidents includes maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics as well as evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources, including network monitoring, incident reports, incident response teams, user complaints, supply chain partners, audit monitoring, physical access monitoring, and user and administrator reports. IR-4 provides information on the types of incidents that are appropriate for monitoring.

Related Controls: AU-6, AU-7, IR-4, IR-6, IR-8, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7.

IR-6 INCIDENT REPORTING

[Priority 2]

Control:

- a. Require personnel to report suspected incidents to the organizational incident response capability immediately but not to exceed one (1) hour after discovery; and
- b. Report incident information to organizational personnel with incident handling responsibilities, and if confirmed, notify the CSO, SIB Chief, or Interface Agency Official.

Discussion: The types of incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Incident information can inform risk assessments, control effectiveness assessments, security requirements for acquisitions, and selection criteria for technology products.

Related Controls: CM-6, CP-2, IR-4, IR-5, IR-8.

Control Enhancements:

(1) INCIDENT REPORTING | AUTOMATED REPORTING

[Existing] [Priority 2]

Control:

Report incidents using automated mechanisms.

Discussion: The recipients of incident reports are specified in IR-6b. Automated reporting mechanisms include email, posting on websites (with automatic updates), and automated incident response tools and programs.

Related Controls: IR-7.

(3) INCIDENT REPORTING | SUPPLY CHAIN COORDINATION

[Priority 2]

Control:

Provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident.

Discussion: Organizations involved in supply chain activities include product developers, system integrators, manufacturers, packagers, assemblers, distributors, vendors, and resellers. Entities that provide supply chain governance include the Federal Acquisition Security Council (FASC). Supply chain incidents include compromises or breaches that involve information technology products, system components, development processes or personnel, distribution processes, or warehousing facilities. Organizations determine the appropriate information to share and consider the value gained from informing external organizations about supply chain incidents, including the ability to improve processes or to identify the root cause of an incident.

Related Controls: SR-8.

IR-7 INCIDENT RESPONSE ASSISTANCE

[Existing] [Priority 3]

Control:

Provide an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the system for the handling and reporting of incidents.

Discussion: Incident response support resources provided by organizations include help desks, assistance groups, automated ticketing systems to open and track incident response tickets, and access to forensics services or consumer redress services, when required.

Related Controls: AT-2, AT-3, IR-4, IR-6, IR-8, SA-9.

Control Enhancements:

(1) INCIDENT RESPONSE ASSISTANCE | AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION AND SUPPORT

[Priority 3]

Control:

Increase the availability of incident response information and support using automated mechanisms described in the discussion.

Discussion: Automated mechanisms can provide a push or pull capability for users to obtain incident response assistance. For example, individuals may have access to a website to query the assistance capability, or the assistance capability can proactively send incident response information to users (general distribution or targeted) as part of increasing understanding of current response capabilities and support.

If the automated mechanisms include external assistance that will give unescorted physical or logical access to CJI, it is imperative to ensure that the appropriate controls/procedures (CJIS Security Addendum/Outsourcing Standard) are in place. Examples would include Cyber Incident Response Vendors (IT Security/Law Firms).

Related Controls: None.

IR-8 INCIDENT RESPONSE PLAN

[Existing] [Priority 2]

Control:

- a. Develop an incident response plan that:
 1. Provides the organization with a roadmap for implementing its incident response capability;

2. Describes the structure and organization of the incident response capability;
 3. Provides a high-level approach for how the incident response capability fits into the overall organization;
 4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
 5. Defines reportable incidents;
 6. Provides metrics for measuring the incident response capability within the organization;
 7. Defines the resources and management support needed to effectively maintain and mature an incident response capability;
 8. Addresses the sharing of incident information;
 9. Is reviewed and approved by the organization's/agency's executive leadership annually; and
 10. Explicitly designates responsibility for incident response to organizational personnel with incident reporting responsibilities and CSO or CJIS WAN Official.
- b. Distribute copies of the incident response plan to organizational personnel with incident handling responsibilities;
 - c. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing;
 - d. Communicate incident response plan changes to organizational personnel with incident handling responsibilities; and
 - e. Protect the incident response plan from unauthorized disclosure and modification.

Discussion: It is important that organizations develop and implement a coordinated approach to incident response. Organizational mission and business functions determine the structure of incident response capabilities. As part of the incident response capabilities, organizations consider the coordination and sharing of information with external organizations, including external service providers and other organizations involved in the supply chain. For incidents involving personally identifiable information (i.e., breaches), include a process to determine whether notice to oversight organizations or affected individuals is appropriate and provide that notice accordingly.

Related Controls: AC-2, CP-2, CP-4, IR-4, IR-7, PE-6, PL-2, SA-15, SI-12, SR-8.

Control Enhancements:

(1) INCIDENT RESPONSE PLAN | BREACHES

[Priority 2]

Control:

Include the following in the Incident Response Plan for breaches involving personally identifiable information:

- a. A process to determine if notice to individuals or other organizations, including oversight organizations, is needed;
- b. An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms; and
- c. Identification of applicable privacy requirements.

Discussion: Organizations may be required by law, regulation, or policy to follow specific procedures relating to breaches, including notice to individuals, affected organizations, and oversight bodies; standards of harm; and mitigation or other specific requirements.

Figure 11 – Incident Response Process Initiated by an Incident in a Local Police Department

A state ISO received a notification from a local police department that suspicious network activity from a known botnet was detected on their network. The state ISO began the process of collecting all pertinent information about this incident, e.g., incident date/time, points-of-contact, systems affected, nature of the incident, actions taken, etc. and requested that the local police department confirm that their malware signatures were up to date. The state ISO contacted both the FBI CJIS ISO and state CSO to relay the preliminary details of this incident. The FBI CJIS ISO instructed the involved parties to continue their investigation and to submit an incident response form once all the information had been gathered. The FBI CJIS ISO contacted the lead for the FBI CSIRC to inform them that an incident response form was forthcoming. The state ISO gathered the remainder of the information from the local police department and submitted a completed incident response form to the FBI CJIS ISO who subsequently provided it to the FBI CSIRC. The FBI CSIRC notified the Department of Justice Computer Incident Response Team (DOJCIRT). The state ISO continued to monitor the situation, passing relevant details to the FBI CJIS ISO, ultimately determining that the botnet was eliminated from the local police department's infrastructure. Subsequent investigations determined that the botnet was restricted to the department's administrative infrastructure and thus no CJI was compromised.

MAINTENANCE (MA)

MA-1 POLICY AND PROCEDURES

[Priority 2]

Control:

- a. Develop, document, and disseminate to organizational personnel with system maintenance responsibilities:
 1. Agency-level maintenance policy that:
 - (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 - (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
 2. Procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls;
- b. Designate an individual with security responsibilities to manage the development, documentation, and dissemination of the maintenance policy and procedures; and
- c. Review and update the current maintenance:
 1. Policy annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI; and
 2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.

Discussion: Maintenance policy and procedures address the controls in the MA family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of maintenance policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to maintenance policy and procedures assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PS-8, SI-12.

MA-2 CONTROLLED MAINTENANCE

[Priority 3]

Control:

- a. Schedule, document, and review records of maintenance, repair, and replacement on system components in accordance with manufacturer or vendor specifications and/or organizational requirements;
- b. Approve and monitor all maintenance activities, whether performed on site or remotely and whether the system or system components are serviced on site or removed to another location;
- c. Require that organizational personnel with information security and privacy responsibilities explicitly approve the removal of the system or system components from organizational facilities for off-site maintenance, repair, or replacement;
- d. Sanitize equipment to remove information from associated media prior to removal from organizational facilities for off-site maintenance, repair, replacement, or destruction;
- e. Check all potentially impacted controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions; and
- f. Include the following information in organizational maintenance records:
 1. Component name
 2. Component serial number
 3. Date/time of maintenance
 4. Maintenance performed
 5. Name(s) of entity performing maintenance including escort if required.

Discussion: Controlling system maintenance addresses the information security aspects of the system maintenance program and applies to all types of maintenance to system components conducted by local or nonlocal entities. Maintenance includes peripherals such as scanners, copiers, and printers. Information necessary for creating effective maintenance records includes the date and time of maintenance, a description of the maintenance performed, names of the individuals or group performing the maintenance, name of the escort, and system components or equipment that are removed or replaced. Organizations consider supply chain-related risks associated with replacement components for systems.

Related Controls: CM-2, CM-3, CM-4, CM-5, CM-8, MA-4, MP-6, PE-16, SI-2, SR-3, SR-11.

MA-3 MAINTENANCE TOOLS

[Priority 4]

Control:

- a. Approve, control, and monitor the use of system maintenance tools; and
- b. Review previously approved system maintenance tools prior to each use.

Discussion: Approving, controlling, monitoring, and reviewing maintenance tools address security-related issues associated with maintenance tools that are not within system authorization boundaries and are used specifically for diagnostic and repair actions on organizational systems. Organizations have flexibility in determining roles for the approval of maintenance tools and how that approval is documented. A periodic review of maintenance tools facilitates the withdrawal of approval for outdated, unsupported, irrelevant, or no-longer- used tools. Maintenance tools can include hardware, software, and firmware items and may be pre-installed, brought in with maintenance personnel on media, cloud-based, or downloaded from a website. Such tools can be vehicles for transporting malicious code, either intentionally or unintentionally, into a facility and subsequently into systems. Maintenance tools can include hardware and software diagnostic test equipment and packet sniffers. The hardware and software components that support maintenance and are a part of the system (including the software implementing utilities such as “ping,” “ls,” “ipconfig,” or the hardware and software implementing the monitoring port of an Ethernet switch) are not addressed by maintenance tools.

Related Controls: MA-2, PE-16.

Control Enhancements:

(1) MAINTENANCE TOOLS | INSPECT TOOLS

[Priority 4]

Control:

Inspect the maintenance tools used by maintenance personnel for improper or unauthorized modifications.

Discussion: Maintenance tools can be directly brought into a facility by maintenance personnel or downloaded from a vendor’s website. If, upon inspection of the maintenance tools, organizations determine that the tools have been modified in an improper manner or the tools contain malicious code, the incident is handled consistent with organizational policies and procedures for incident handling.

Related Controls: SI-7.

(2) MAINTENANCE TOOLS | INSPECT MEDIA

[Priority 4]

Control:

Check media containing diagnostic and test programs for malicious code before the media are used in the system.

Discussion: If, upon inspection of media containing maintenance, diagnostic, and test programs, organizations determine that the media contains malicious code, the incident is handled consistent with organizational incident handling policies and procedures.

Related Controls: SI-3.

(3) MAINTENANCE TOOLS | PREVENT UNAUTHORIZED REMOVAL

[Priority 4]

Control:

Prevent the removal of maintenance equipment containing organizational information by:

- a. Verifying that there is no organizational information contained on the equipment;
- b. Sanitizing or destroying the equipment;
- c. Retaining the equipment within the facility; or
- d. Obtaining an exemption from organizational personnel with system maintenance responsibilities explicitly authorizing removal of the equipment from the facility.

Discussion: Organizational information includes all information owned by organizations and any information provided to organizations for which the organizations serve as information stewards.

Related Controls: MP-6.

MA-4 NONLOCAL MAINTENANCE

[Priority 3]

Control:

- a. Approve and monitor nonlocal maintenance and diagnostic activities;
- b. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system;
- c. Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions;
- d. Maintain records for nonlocal maintenance and diagnostic activities; and
- e. Terminate session and network connections when nonlocal maintenance is completed.

Discussion: Nonlocal maintenance and diagnostic activities are conducted by individuals who communicate through either an external or internal network. Local maintenance and diagnostic activities are carried out by individuals who are physically present at the system location and not communicating across a network connection. Authentication techniques used to establish nonlocal maintenance and diagnostic sessions reflect the network access requirements in IA-2. Strong authentication requires authenticators that are resistant to replay attacks and employ multi-factor authentication. Strong authenticators include PKI where certificates are stored on a token protected by a password, passphrase, or biometric. Enforcing requirements in MA-4 is accomplished, in part, by other controls.

Related Controls: AC-2, AC-3, AC-6, AC-17, AU-2, AU-3, IA-2, IA-4, IA-5, IA-8, MA-2, MA-5, PL-2, SC-7, SC-10.

MA-5 MAINTENANCE PERSONNEL

[Priority 3]

Control:

- a. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel;

- b. Verify that non-escorted personnel performing maintenance on the system possess the required access authorizations; and
- c. Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

Discussion: Maintenance personnel refers to individuals who perform hardware or software maintenance on organizational systems, while PE-2 addresses physical access for individuals whose maintenance duties place them within the physical protection perimeter of the systems. Technical competence of supervising individuals relates to the maintenance performed on the systems, while having required access authorizations refers to maintenance on and near the systems. Individuals not previously identified as authorized maintenance personnel—such as information technology manufacturers, vendors, systems integrators, and consultants—may require privileged access to organizational systems, such as when they are required to conduct maintenance activities with little or no notice. Based on organizational assessments of risk, organizations may issue temporary credentials to these individuals. Temporary credentials may be for one-time use or for very limited time periods.

Related Controls: AC-2, AC-3, AC-5, AC-6, IA-2, IA-8, MA-4, MP-2, PE-2, PE-3, PS-7, RA-3.

MA-6 TIMELY MAINTENANCE

[Priority 3]

Control:

Obtain maintenance support and/or spare parts for critical system components that process, store, and transmit CJI within agency-defined recovery time and recovery point objectives of failure.

Discussion: Organizations specify the system components that result in increased risk to organizational operations and assets, individuals, other organizations, or the Nation when the functionality provided by those components is not operational. Organizational actions to obtain maintenance support include having appropriate contracts in place.

Related Controls: CM-8, CP-2, CP-7, RA-7, SA-15, SR-2, SR-3.

MEDIA PROTECTION (MP)

Documented and implemented media protection policies and procedures ensure that access to digital and non-digital media in all forms is restricted to authorized individuals using authorized methods and processes.

MP-1 POLICY AND PROCEDURES

[Existing] [Priority 2]

Control:

- a. Develop, document, and disseminate to authorized individuals:
 1. Agency-level media protection policy that:
 - (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance; and
 - (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
 2. Procedures to facilitate the implementation of the media protection policy and the associated media protection controls;
- b. Designate an individual with security responsibilities to manage the development, documentation, and dissemination of the media protection policy and procedures; and
- c. Review and update the current media protection:
 1. Policy at least annually and following any security incidents involving digital and/or non-digital media; and
 2. Procedures at least annually and following any security incidents involving digital and/or non-digital media.

Discussion: Media protection policy and procedures address the controls in the MP family that are implemented within systems and agencies. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of media protection policy and procedures. Security and privacy program policies and procedures at the agency level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of agencies. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to media protection policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an agency policy or procedure.

Related Controls: PS-8, SI-12.

MP-2 MEDIA ACCESS

[Existing] [Priority 2]

Control:

Restrict access to digital and non-digital media to authorized individuals.

Discussion: System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state, magnetic), compact discs, and digital versatile discs. Non-digital media includes paper and microfilm. Denying access to hard copies of case file information stored in a locked filing cabinet is an example of restricting access to non-digital media. Limiting access to the design specifications stored on compact discs in the media library to individuals on the system development team is an example of restricting access to digital media.

Related Controls: AC-19, AU-9, CP-2, CP-9, CP-10, MA-5, MP-4, MP-6, PE-2, PE-3, SC-12, SC-13, SI-12.

MP-3 MEDIA MARKING

[Priority 3]

Control:

- a. Mark system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and
- b. Exempt digital and non-digital media containing CJI from marking if the media remain within physically secure locations or controlled areas.

Discussion: Security marking refers to the application or use of human-readable security attributes. Digital media includes diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state, magnetic), flash drives, compact discs, and digital versatile discs. Non-digital media includes paper and microfilm. Controlled unclassified information (CUI) is defined by the National Archives and Records Administration (NARA) along with the appropriate safeguarding and dissemination requirements for such information and is codified in [32 CFR 2002]. Security markings are generally not required for media that contains information determined by agencies to be in the public domain or to be publicly releasable. Some agencies may require markings for public information indicating that the information is publicly releasable. System media marking reflects applicable laws, executive orders, directives, policies, regulations, standards, and guidelines. Executive Order 13556 mandates the marking of CUI. The following categories of CJI fall under the designated NARA categories which direct marking as indicated.

1. Biometric Data—data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population. Used to identify individuals, to include: fingerprints, palm prints, iris scans, and facial recognition data. NARA CUI Category: Sensitive Personally Identifiable Information. NARA Banner Marking: CUI

- ~~2. Identity History Data—textual data that corresponds with an individual’s biometric data, providing a history of criminal and/or civil events for the identified individual. NARA CUI Category: Criminal History Records Information. NARA Banner Marking: CUI//SP-CHRI~~
- ~~3. Biographic Data—information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case. NARA CUI Category: General Law Enforcement. NARA Banner Marking: CUI~~
- ~~4. Property Data—information about vehicles and property associated with crime when accompanied by any personally identifiable information (PII). NARA CUI Category: General Law Enforcement. NARA Banner Marking: CUI~~
- ~~5. Case/Incident History—information about the history of criminal incidents. NARA CUI Category: General Law Enforcement. NARA Banner Marking: CUI~~

~~[32 CFR 2002] states the CUI Program prohibits using markings or practices not included in this part or the CUI Registry. If legacy markings remain on information, the legacy markings are void and no longer indicate that the information is protected or that it is or qualifies as CUI.~~

~~Related Controls: CP-9, MP-5, SI-12.~~

MP-4 MEDIA STORAGE

[Existing] [Priority 2]

Control:

- a. Physically control and securely store digital and non-digital media within physically secure locations or controlled areas and encrypt CJI on digital media when physical and personnel restrictions are not feasible; and
- b. Protect system media types defined in MP-4a until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

Discussion: System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state, magnetic), compact discs, and digital versatile discs. Non-digital media includes paper and microfilm. Physically controlling stored media includes conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the library, and maintaining accountability for stored media. Secure storage includes a locked drawer, desk, or cabinet or a controlled media library. The type of media storage is commensurate with the security category or classification of the information on the media. Controlled areas are spaces that provide physical and procedural controls to meet the requirements established for protecting information and systems. Fewer controls may be needed for media that contains information determined to be in the public domain, publicly releasable, or have limited adverse impacts on agencies, operations, or individuals if accessed by other than authorized personnel. In these situations, physical access controls provide adequate protection.

Related Controls: AC-19, CP-2, CP-6, CP-9, CP-10, MP-2, MP-7, PE-3, PL-2, SC-12, SC-13, SC-28, SI-12.

MP-5 MEDIA TRANSPORT

[Existing] [Priority 2]

Control:

- a. Protect and control digital and non-digital media to help prevent compromise of the data during transport outside of the physically secure locations or controlled areas using encryption, as defined in SC-13 and SC-28 of this Policy. Physical media will be protected at the same level as the information would be protected in electronic form. Restrict the activities associated with transport of electronic and physical media to authorized personnel;
- b. Maintain accountability for system media during transport outside of the physically secure location or controlled areas;
- c. Document activities associated with the transport of system media; and
- d. Restrict the activities associated with the transport of system media to authorized personnel.

Discussion: System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state and magnetic), compact discs, and digital versatile discs. Non-digital media includes microfilm and paper. Controlled areas are spaces for which agencies provide physical or procedural controls to meet requirements established for protecting information and systems. Controls to protect media during transport include cryptography and locked containers. Cryptographic mechanisms can provide confidentiality and integrity protections depending on the mechanisms implemented. Activities associated with media transport include releasing media for transport, ensuring that media enters the appropriate transport processes, and the actual transport. Authorized transport and courier personnel may include individuals external to the agency. Maintaining accountability of media during transport includes restricting transport activities to authorized personnel and tracking and/or obtaining records of transport activities as the media moves through the transportation system to prevent and detect loss, destruction, or tampering. Agencies establish documentation requirements for activities associated with the transport of system media in accordance with agency assessments of risk. Agencies maintain the flexibility to define record-keeping methods for the different types of media transport as part of a system of transport-related records.

Related Controls: AC-7, AC-19, CP-2, CP-9, MP-3, MP-4, PE-16, PL-2, SC-12, SC-13, SC-28.

MP-6 MEDIA SANITIZATION

[Existing] [Priority 2]

Control:

- a. Sanitize or destroy digital and non-digital media prior to disposal, release out of agency control, or release for reuse using overwrite technology at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media will be destroyed (cut up, shredded, etc.). Physical media will be securely disposed of

when no longer needed for investigative or security purposes, whichever is later. Physical media will be destroyed by crosscut shredding or incineration; and

- b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

Discussion: Media sanitization applies to all digital and non-digital system media subject to disposal or reuse, whether or not the media is considered removable. Examples include digital media in scanners, copiers, printers, notebook computers, workstations, network components, mobile devices, and non-digital media (e.g., paper and microfilm). The sanitization process removes information from system media such that the information cannot be retrieved or reconstructed. Sanitization techniques—including clearing, purging, cryptographic erase, de-identification of personally identifiable information, and destruction—prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal. Agencies determine the appropriate sanitization methods, recognizing that destruction is sometimes necessary when other methods cannot be applied to media requiring sanitization.

Agencies use discretion on the employment of approved sanitization techniques and procedures for media that contains information deemed to be in the public domain or publicly releasable or information deemed to have no adverse impact on agencies or individuals if released for reuse or disposal. Sanitization of non-digital media includes destruction, removing a classified appendix from an otherwise unclassified document, or redacting selected sections or words from a document by obscuring the redacted sections or words in a manner equivalent in effectiveness to removing them from the document. NSA standards and policies control the sanitization process for media that contains classified information. NARA policies control the sanitization process for controlled unclassified information.

Related Controls: AC-3, AC-7, AU-11, MA-2, MA-3, MA-4, MA-5, SI-12, SR-11.

MP-7 MEDIA USE

[Existing] [Priority 2]

Control:

- a. Restrict the use of digital and non-digital media on agency owned systems that have been approved for use in the storage, processing, or transmission of criminal justice information by using technical, physical, or administrative controls (examples below); and
- b. Prohibit the use of personally owned digital media devices on all agency owned or controlled systems that store, process, or transmit criminal justice information; and
- c. Prohibit the use of digital media devices on all agency owned or controlled systems that store, process, or transmit criminal justice information when such devices have no identifiable owner.

Examples of technical controls: port disabling, access control lists (ACL), security groups, group policy objects (GPO), mobile device management (MDM).

Example of physical control: locked server cage, disconnect CD-ROM drive in PC, remove USB port.

Example of administrative controls: the agency's electronic media policy defining how flash drives are to be used within the agency rules of behavior.

Discussion: System media includes both digital and non-digital media. Digital media includes diskettes, magnetic tapes, flash drives, compact discs, digital versatile discs, and removable hard disk drives. Non-digital media includes paper and microfilm. Media use protections also apply to mobile devices with information storage capabilities. In contrast to MP-2, which restricts user access to media, MP-7 restricts the use of certain types of media on systems, for example, restricting or prohibiting the use of flash drives or external hard disk drives. Agencies use technical and nontechnical controls to restrict the use of system media. Agencies may restrict the use of portable storage devices, for example, by using physical cages on workstations to prohibit access to certain external ports or disabling or removing the ability to insert, read, or write to such devices. Agencies may also limit the use of portable storage devices to only approved devices, including devices provided by the agency, devices provided by other approved agencies, and devices that are not personally owned. Finally, agencies may restrict the use of portable storage devices based on the type of device, such as by prohibiting the use of writeable, portable storage devices and implementing this restriction by disabling or removing the capability to write to such devices. Requiring identifiable owners for storage devices reduces the risk of using such devices by allowing agencies to assign responsibility for addressing known vulnerabilities in the devices.

Related Controls: AC-19, AC-20, PL-4.

Figure 12 – A Local Police Department's Media Management Policies

A local police department implemented a replacement CAD system that integrated to their state's CSA and was authorized to process CJI. The police department contracted with an off-site media manager to store backups of their data in the contractor's vaults, but the contractor was not authorized to process or store CJI. To ensure the confidentiality of the police department's data while outside its perimeter, they encrypted all data going to the contractor with an encryption product that is FIPS 140-2 certified. The police department rotated and reused media through the contractor's vaults periodically, and when it required destruction, the police department incinerated the media to irreversibly destroy any data on it.

PHYSICAL AND ENVIRONMENTAL PROTECTION (PE)

PE-1 POLICY AND PROCEDURES

[Priority 2]

Control:

- a. Develop, document, and disseminate to organizational personnel with physical and environmental protection responsibilities:
 1. Agency-level physical and environmental protection policy that:
 - (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 - (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
 2. Procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental protection controls;
- b. Designate organizational personnel with information security responsibilities to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures; and
- c. Review and update the current physical and environmental protection:
 1. Policy annually and following any physical, environmental, or security related incidents involving CJI or systems used to process, store, or transmit CJI; and
 2. Procedures annually and following any physical, environmental, or security related incidents involving CJI or systems used to process, store, or transmit CJI.

Discussion: Physical and environmental protection policy and procedures address the controls in the PE family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of physical and environmental protection policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to physical and environmental protection policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: AT-3, PS-8, SI-12.

PE-2 PHYSICAL ACCESS AUTHORIZATIONS

[Existing] [Priority 2]

Control:

- a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides;
- b. Issue authorization credentials for facility access;
- c. Review the access list detailing authorized facility access by individuals annually and when personnel changes occur; and
- d. Remove individuals from the facility access list when access is no longer required.

Discussion: Physical access authorizations apply to employees and visitors. Individuals with permanent physical access authorization credentials are not considered visitors. Authorization credentials include ID badges, identification cards, and smart cards. Organizations determine the strength of authorization credentials needed consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Physical access authorizations may not be necessary to access certain areas within facilities that are designated as publicly accessible.

Related Controls: AT-3, AU-9, IA-4, MA-5, MP-2, PE-3, PE-4, PE-5, PE-8, PS-3, PS-4, PS-5, PS-6.

PE-3 PHYSICAL ACCESS CONTROL

[Existing] [Priority 2]

Control:

- a. Enforce physical access authorizations by:
 1. Verifying individual access authorizations before granting access to the facility; and
 2. Controlling ingress and egress to the facility using agency-implemented procedures and controls;
- b. Maintain physical access audit logs for the physically secure location and agency-defined sensitive areas;
- c. Control access to areas within the facility designated as non-publicly accessible by implementing physical access devices including, but not limited to keys, locks, combinations, biometric readers, placards, and/or card readers;
- d. Escort visitors and control visitor activity in all physically secure locations;
- e. Secure keys, combinations, and other physical access devices;
- f. Inventory all agency-issued physical access devices annually; and
- g. Change combinations and keys when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated.

h. If the above conditions cannot be met refer to the requirements listed in PE-17.

Discussion: Physical access control applies to employees and visitors. Individuals with permanent physical access authorizations are not considered visitors. Physical access controls for publicly accessible areas may include physical access control logs/records, guards, or physical access devices and barriers to prevent movement from publicly accessible areas to non-public areas.

Organizations determine the types of guards needed, including professional security staff, system users, or administrative staff. Physical access devices include keys, locks, combinations, biometric readers, and card readers. Physical access control systems comply with applicable laws, executive orders, directives, policies, regulations, standards, and guidelines. Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural, automated, or some combination thereof. Physical access points can include facility access points, interior access points to systems that require supplemental access controls, or both. Components of systems may be in areas designated as publicly accessible with organizations controlling access to the components.

Related Controls: AT-3, AU-2, AU-6, AU-9, CP-10, IA-3, IA-8, MA-5, MP-2, MP-4, PE-2, PE-4, PE-5, PE-8, PS-2, PS-3, PS-6, PS-7, RA-3, SC-28, SI-4, SR-3.

PE-4 ACCESS CONTROL FOR TRANSMISSION

[Existing] [Priority 2]

Control:

Control physical access to information system distribution and transmission lines and devices within organizational facilities using agency-implemented procedures and controls.

Discussion: Security controls applied to system distribution and transmission lines prevent accidental damage, disruption, and physical tampering. Such controls may also be necessary to prevent eavesdropping or modification of unencrypted transmissions. Security controls used to control physical access to system distribution and transmission lines include disconnected or locked spare jacks, locked wiring closets, protection of cabling by conduit or cable trays, and wiretapping sensors.

Related Controls: AT-3, IA-4, MP-2, MP-4, PE-2, PE-3, PE-5, PE-9, SC-7, SC-8.

PE-5 ACCESS CONTROL FOR OUTPUT DEVICES

[Existing] [Priority 3]

Control:

Control physical access to output from monitors, printers, scanners, audio devices, facsimile machines, and copiers to prevent unauthorized individuals from obtaining the output.

Discussion: Controlling physical access to output devices includes placing output devices in locked rooms or other secured areas with keypad or card reader access controls and allowing access to authorized individuals only, placing output devices in locations that can be monitored

by personnel, installing monitor or screen filters, and using headphones. Examples of output devices include monitors, printers, scanners, audio devices, facsimile machines, and copiers.

Related Controls: PE-2, PE-3, PE-4.

PE-6 MONITORING PHYSICAL ACCESS

[Existing] [Priority 2]

Control:

- a. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents;
- b. Review physical access logs quarterly and upon occurrence of any physical, environmental, or security-related incidents involving CJI or systems used to process, store, or transmit CJI; and
- c. Coordinate results of reviews and investigations with the organizational incident response capability.

Discussion: Physical access monitoring includes publicly accessible areas within organizational facilities. Examples of physical access monitoring include the employment of guards, video surveillance equipment (i.e., cameras), and sensor devices. Reviewing physical access logs can help identify suspicious activity, anomalous events, or potential threats. The reviews can be supported by audit logging controls, such as AU-2, if the access logs are part of an automated system. Organizational incident response capabilities include investigations of physical security incidents and responses to the incidents. Incidents include security violations or suspicious physical access activities. Suspicious physical access activities include accesses outside of normal work hours, repeated accesses to areas not normally accessed, accesses for unusual lengths of time, and out-of-sequence accesses.

Related Controls: AU-2, AU-6, AU-9, AU-12, CA-7, CP-10, IR-4, IR-8.

Control Enhancements:

(1) MONITORING PHYSICAL ACCESS | INTRUSION ALARMS AND SURVEILLANCE EQUIPMENT

[Existing] [Priority 2]

Control:

Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment.

Discussion: Physical intrusion alarms can be employed to alert security personnel when unauthorized access to the facility is attempted. Alarm systems work in conjunction with physical barriers, physical access control systems, and security guards by triggering a response when these other forms of security have been compromised or breached. Physical intrusion alarms can include different types of sensor devices, such as motion sensors, contact sensors, and

broken glass sensors. Surveillance equipment includes video cameras installed at strategic locations throughout the facility.

Related Controls: None.

PE-8 VISITOR ACCESS RECORDS

[Priority 4]

Control:

- a. Maintain visitor access records to the facility where the system resides for one (1) year;
- b. Review visitor access records quarterly; and
- c. Report anomalies in visitor access records to organizational personnel with physical and environmental protection responsibilities and organizational personnel with information security responsibilities.

Discussion: Visitor access records include the names and organizations of individuals visiting, visitor signatures, forms of identification, dates of access, entry and departure times, purpose of visits, and the names and organizations of individuals visited. Access record reviews determine if access authorizations are current and are still required to support organizational mission and business functions. Access records are not required for publicly accessible areas.

Related Controls: PE-2, PE-3, PE-6.

Control Enhancements:

(3) VISITOR ACCESS RECORDS | LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS

[Priority 4]

Control:

Limit personally identifiable information contained in visitor access records to the minimum PII necessary to achieve the purpose for which it is collected (see Section 4.3).

Note: Access to visitor access records is restricted to authorized agency personnel.

Discussion: Organizations may have requirements that specify the contents of visitor access records. Limiting personally identifiable information in visitor access records when such information is not needed for operational purposes helps reduce the level of privacy risk created by a system.

Related Controls: RA-3, SA-8.

PE-9 POWER EQUIPMENT AND CABLING

[Priority 2]

Control:

Protect power equipment and power cabling for the system from damage and destruction.

Note: This control only applies to data centers as defined in Appendix A Terms and Definitions.

Discussion: Organizations determine the types of protection necessary for the power equipment and cabling employed at different locations that are both internal and external to organizational facilities and environments of operation. Types of power equipment and cabling include internal cabling and uninterruptible power sources in offices or data centers, generators and power cabling outside of buildings, and power sources for self-contained components such as satellites, vehicles, and other deployable systems.

Related Controls: PE-4.

PE-10 EMERGENCY SHUTOFF

[Priority 2]

Control:

- a. Provide the capability of shutting off power to all information systems in emergency situations;
- b. Place emergency shutoff switches or devices in easily accessible locations to facilitate access for authorized personnel; and
- c. Protect emergency power shutoff capability from unauthorized activation.

Note: This control only applies to data centers as defined in Appendix A Terms and Definitions.

Discussion: Emergency power shutoff primarily applies to organizational facilities that contain concentrations of system resources, including data centers, mainframe computer rooms, server rooms, and areas with computer-controlled machinery.

Related Controls: PE-15.

PE-11 EMERGENCY POWER

[Priority 2]

Control:

Provide an uninterruptible power supply to facilitate an orderly shutdown of the information system or transition of the information system to an alternate power source in the event of a primary power source loss.

Note: This control only applies to data centers as defined in Appendix A Terms and Definitions.

Discussion: An uninterruptible power supply (UPS) is an electrical system or mechanism that provides emergency power when there is a failure of the main power source. A UPS is typically used to protect computers, data centers, telecommunication equipment, or other electrical equipment where an unexpected power disruption could cause injuries, fatalities, serious mission or business disruption, or loss of data or information. A UPS differs from an emergency power system or backup generator in that the UPS provides near-instantaneous protection from

unanticipated power interruptions from the main power source by providing energy stored in batteries, supercapacitors, or flywheels. The battery duration of a UPS is relatively short but provides sufficient time to start a standby power source, such as a backup generator, or properly shut down the system.

Related Controls: AT-3, CP-2, CP-7.

PE-12 EMERGENCY LIGHTING

[Priority 2]

Control:

Employ and maintain automatic emergency lighting for the system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

Note: This control only applies to data centers as defined in Appendix A Terms and Definitions.

Discussion: The provision of emergency lighting applies primarily to organizational facilities that contain concentrations of system resources, including data centers, server rooms, and mainframe computer rooms. Emergency lighting provisions for the system are described in the contingency plan for the organization. If emergency lighting for the system fails or cannot be provided, organizations consider alternate processing sites for power-related contingencies.

Related Controls: CP-2, CP-7.

PE-13 FIRE PROTECTION

[Priority 2]

Control:

Employ and maintain fire detection and suppression systems that are supported by an independent energy source.

Note: This control only applies to data centers as defined in Appendix A Terms and Definitions.

Discussion: The provision of fire detection and suppression systems applies primarily to organizational facilities that contain concentrations of system resources, including data centers, server rooms, and mainframe computer rooms. Fire detection and suppression systems that may require an independent energy source include sprinkler systems and smoke detectors. An independent energy source is an energy source, such as a microgrid, that is separate, or can be separated, from the energy sources providing power for the other parts of the facility.

Related Controls: AT-3.

Control Enhancements:

(1) FIRE PROTECTION | DETECTION SYSTEMS — AUTOMATIC ACTIVATION AND NOTIFICATION

[Priority 2]

Control:

Employ fire detection systems that activate automatically and notify organizational personnel with physical and environmental protection responsibilities and police, fire, or emergency medical personnel in the event of a fire.

Note: This control only applies to data centers as defined in Appendix A Terms and Definitions.

Discussion: Organizations can identify personnel, roles, and emergency responders if individuals on the notification list need to have access authorizations or clearances (e.g., to enter to facilities where access is restricted due to the classification or impact level of information within the facility). Notification mechanisms may require independent energy sources to ensure that the notification capability is not adversely affected by the fire.

Related Controls: None.

PE-14 ENVIRONMENTAL CONTROLS

[Priority 2]

Control:

- a. Maintain adequate HVAC levels within the facility where the system resides at recommended system manufacturer levels; and
- b. Monitor environmental control levels continuously.

Note: This control only applies to data centers as defined in Appendix A Terms and Definitions.

Discussion: The provision of environmental controls applies primarily to organizational facilities that contain concentrations of system resources (e.g., data centers, mainframe computer rooms, and server rooms). Insufficient environmental controls, especially in very harsh environments, can have a significant adverse impact on the availability of systems and system components that are needed to support organizational mission and business functions.

Related Controls: AT-3, CP-2.

PE-15 WATER DAMAGE PROTECTION

[Priority 2]

Control:

Protect the system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

Note: This control only applies to data centers as defined in Appendix A Terms and Definitions.

Discussion: The provision of water damage protection primarily applies to organizational facilities that contain concentrations of system resources, including data centers, server rooms,

and mainframe computer rooms. Isolation valves can be employed in addition to or in lieu of master shutoff valves to shut off water supplies in specific areas of concern without affecting entire organizations.

Related Controls: AT-3, PE-10.

PE-16 DELIVERY AND REMOVAL

[Existing] [Priority 3]

Control:

- a. Authorize and control information system-related components entering and exiting the facility; and
- b. Maintain records of the system components.

Discussion: Enforcing authorizations for entry and exit of system components may require restricting access to delivery areas and isolating the areas from the system and media libraries.

Related Controls: CM-3, CM-8, MA-2, MA-3, MP-5, SR-2, SR-3, SR-6.

PE-17 ALTERNATE WORK SITE

[Existing] [Priority 3]

Control:

- a. Determine and document all alternate facilities or locations allowed for use by employees;
- b. Employ the following controls at alternate work sites:
 1. Limit access to the area during CJI processing times to only those personnel authorized by the agency to access or view CJI.
 2. Lock the area, room, or storage container when unattended.
 3. Position information system devices and documents containing CJI in such a way as to prevent unauthorized individuals from access and view.
 4. Follow the encryption requirements found in SC-13 and SC-28 for electronic storage (i.e., data at-rest) of CJI.
- c. Assess the effectiveness of controls at alternate work sites; and
- d. Provide a means for employees to communicate with information security and privacy personnel in case of incidents.

Discussion: Alternate work sites include government facilities or the private residences of employees. While distinct from alternative processing sites, alternate work sites can provide readily available alternate locations during contingency operations. Organizations can define different sets of controls for specific alternate work sites or types of sites depending on the work-related activities conducted at the sites. Implementing and assessing the effectiveness of

organization-defined controls and providing a means to communicate incidents at alternate work sites supports the contingency planning activities of organizations.

Related Controls: AC-17, AC-18, CP-7.

PLANNING (PL)

PL-1 POLICY AND PROCEDURES

[Priority 2]

Control:

- a. Develop, document, and disseminate to organizational personnel with planning responsibilities:
 1. Agency-level planning policy that:
 - (c) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 - (d) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
 2. Procedures to facilitate the implementation of the planning policy and the associated planning controls;
- b. Designate organizational personnel with information security and privacy responsibilities to manage the development, documentation, and dissemination of the planning policy and procedures; and
- c. Review and update the current planning:
 1. Policy annually and following; any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI and
 2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.

Discussion: Planning policy and procedures for the controls in the PL family implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on their development. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission level or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission/business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to planning policy and procedures include, but are not limited to, assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PS-8, SI-12.

PL-2 SYSTEM SECURITY AND PRIVACY PLANS

[Priority 2]

Control:

- a. Develop security and privacy plans for the system that:
 1. Are consistent with the organization's enterprise architecture;
 2. Explicitly define the constituent system components;
 3. Describe the operational context of the system in terms of mission and business processes;
 4. Identify the individuals that fulfill system roles and responsibilities;
 5. Identify the information types processed, stored, and transmitted by the system;
 6. Provide the security categorization of the system, including supporting rationale;
 7. Describe any specific threats to the system that are of concern to the organization;
 8. Provide the results of a privacy risk assessment for systems processing personally identifiable information;
 9. Describe the operational environment for the system and any dependencies on or connections to other systems or system components;
 10. Provide an overview of the security and privacy requirements for the system;
 11. Identify any relevant control baselines or overlays, if applicable;
 12. Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions;
 13. Include risk determinations for security and privacy architecture and design decisions;
 14. Include security- and privacy-related activities affecting the system that require planning and coordination with organizational personnel with system security and privacy planning and plan implementation responsibilities; system developers; organizational personnel with information security and privacy responsibilities; and
 15. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation.
- b. Distribute copies of the plans and communicate subsequent changes to the plans to organizational personnel with system security and privacy planning and plan implementation responsibilities; system developers; organizational personnel with information security and privacy responsibilities;
- c. Review the system security and privacy plans at least annually or when required due to system changes or modifications;
- d. Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments; and
- e. Protect the plans from unauthorized disclosure and modification.

Discussion: System security and privacy plans are scoped to the system and system components within the defined authorization boundary and contain an overview of the security and privacy requirements for the system and the controls selected to satisfy the requirements. The plans describe the intended application of each selected control in the context of the system with a sufficient level of detail to correctly implement the control and to subsequently assess the effectiveness of the control. The control documentation describes how system-specific and hybrid controls are implemented and the plans and expectations regarding the functionality of the system. System security and privacy plans can also be used in the design and development of systems in support of life cycle-based security and privacy engineering processes. System security and privacy plans are living documents that are updated and adapted throughout the system development life cycle (e.g., during capability determination, analysis of alternatives, requests for proposal, and design reviews). The CJISSECPOL describes the different types of requirements that are relevant to organizations during the system development life cycle and the relationship between requirements and controls.

Organizations may develop a single, integrated security and privacy plan or maintain separate plans. Security and privacy plans relate security and privacy requirements to a set of controls and control enhancements. The plans describe how the controls and control enhancements meet the security and privacy requirements but do not provide detailed, technical descriptions of the design or implementation of the controls and control enhancements. Security and privacy plans contain sufficient information (including specifications of control parameter values for selection and assignment operations explicitly or by reference) to enable a design and implementation that is unambiguously compliant with the intent of the plans and subsequent determinations of risk to organizational operations and assets, individuals, other organizations, and the Nation if the plan is implemented.

Security and privacy plans need not be single documents. The plans can be a collection of various documents, including documents that already exist. Effective security and privacy plans make extensive use of references to policies, procedures, and additional documents, including design and implementation specifications where more detailed information can be obtained. The use of references helps reduce the documentation associated with security and privacy programs and maintains the security- and privacy-related information in other established management and operational areas, including enterprise architecture, system development life cycle, systems engineering, and acquisition. Security and privacy plans need not contain detailed contingency plan or incident response plan information but can instead provide—explicitly or by reference—sufficient information to define what needs to be accomplished by those plans.

Security- and privacy-related activities that may require coordination and planning with other individuals or groups within the organization include assessments, audits, inspections, hardware and software maintenance, acquisition and supply chain risk management, patch management, and contingency plan testing. Planning and coordination include emergency and nonemergency (i.e., planned or non-urgent unplanned) situations. The process defined by organizations to plan and coordinate security- and privacy-related activities can also be included in other documents, as appropriate.

Related Controls: AC-2, AC-6, AC-14, AC-17, AC-20, CA-2, CA-3, CA-7, CM-9, CP-2, CP-4, IR-4, IR-8, MA-4, MA-5, MP-4, MP-5, PL-8, PL-10, PL-11, RA-3, RA-9, SA-5, SA-22, SI-12, SR-2.

PL-4 RULES OF BEHAVIOR

[Priority 3]

Control:

- a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy;
- b. Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system;
- c. Review and update the rules of behavior at least annually; and
- d. Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge annually, or when the rules are revised or updated.

Discussion: Rules of behavior represent a type of access agreement for organizational users. Other types of access agreements include nondisclosure agreements, conflict-of-interest agreements, and acceptable use agreements (see PS-6). Organizations consider rules of behavior based on individual user roles and responsibilities and differentiate between rules that apply to privileged users and rules that apply to general users. Establishing rules of behavior for some types of non-organizational users, including individuals who receive information from federal systems, is often not feasible given the large number of such users and the limited nature of their interactions with the systems. Rules of behavior for organizational and non-organizational users can also be established in AC-8. The related controls section provides a list of controls that are relevant to organizational rules of behavior. PL-4b, the documented acknowledgment portion of the control, may be satisfied by the literacy training and awareness and role-based training programs conducted by organizations if such training includes rules of behavior. Documented acknowledgements for rules of behavior include electronic or physical signatures and electronic agreement check boxes or radio buttons.

Related Controls: AC-2, AC-6, AC-8, AC-17, AC-18, AC-19, AC-20, AT-2, AT-3, CM-11, IA-2, IA-4, IA-5, MP-7, PS-6, PS-8, SA-5, SI-12.

Control Enhancements:

(1) RULES OF BEHAVIOR | SOCIAL MEDIA AND EXTERNAL SITE/APPLICATION USAGE RESTRICTIONS

[Priority 3]

Control:

Include in the rules of behavior, restrictions on:

- a. Use of social media, social networking sites, and external sites/applications;
- b. Posting organizational information on public websites; and
- c. Use of organization-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications.

Discussion: Social media, social networking, and external site/application usage restrictions address rules of behavior related to the use of social media, social networking, and external sites when organizational personnel are using such sites for official duties or in the conduct of official business, when organizational information is involved in social media and social networking transactions, and when personnel access social media and networking sites from organizational systems. Organizations also address specific rules that prevent unauthorized entities from obtaining non-public organizational information from social media and networking sites either directly or through inference. Non-public information includes personally identifiable information and system account information.

Related Controls: AC-22.

PL-8 SECURITY AND PRIVACY ARCHITECTURES

[Priority 2]

Control:

- a. Develop security and privacy architectures for the system that:
 1. Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information;
 2. Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals;
 3. Describe how the architectures are integrated into and support the enterprise architecture; and
 4. Describe any assumptions about, and dependencies on, external systems and services;
- b. Review and update the architectures at least annually or when changes to the system or its environment occur to reflect changes in the enterprise architecture; and
- c. Reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and acquisitions.

Discussion: The security and privacy architectures at the system level are consistent with the organization-wide security and privacy architectures are integral to and developed as part of the enterprise architecture. The architectures include an architectural description, the allocation of security and privacy functionality (including controls), security- and privacy-related information for external interfaces, information being exchanged across the interfaces, and the protection mechanisms associated with each interface. The architectures can also include other information, such as user roles and the access privileges assigned to each role; security and privacy requirements; types of information processed, stored, and transmitted by the system; supply chain risk management requirements; restoration priorities of information and system services; and other protection needs.

[SP 800-160-1] provides guidance on the use of security architectures as part of the system development life cycle process. Security and privacy architectures are reviewed and updated throughout the system development life cycle, from analysis of alternatives through review of the

proposed architecture in the RFP responses to the design reviews before and during implementation (e.g., during preliminary design reviews and critical design reviews).

In today's modern computing architectures, it is becoming less common for organizations to control all information resources. There may be key dependencies on external information services and service providers. Describing such dependencies in the security and privacy architectures is necessary for developing a comprehensive mission and business protection strategy. Establishing, developing, documenting, and maintaining under configuration control a baseline configuration for organizational systems is critical to implementing and maintaining effective architectures. The development of the architectures is coordinated with the senior agency information security officer and the senior agency official for privacy to ensure that the controls needed to support security and privacy requirements are identified and effectively implemented. In many circumstances, there may be no distinction between the security and privacy architecture for a system. In other circumstances, security objectives may be adequately satisfied, but privacy objectives may only be partially satisfied by the security requirements. In these cases, consideration of the privacy requirements needed to achieve satisfaction will result in a distinct privacy architecture. The documentation, however, may simply reflect the combined architectures.

Related Controls: CM-2, CM-6, PL-2, PL-7, PL-9, PM-5, RA-9, SA-3, SA-5, SA-8, SC-7.

PL-9 CENTRAL MANAGEMENT

[Priority 4]

Control:

The CJISSECPOL is centrally managed by the FBI CJIS ISO.

Discussion: Central management refers to organization-wide management and implementation of selected controls and processes. This includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed controls and processes. As the central management of controls is generally associated with the concept of common (inherited) controls, such management promotes and facilitates standardization of control implementations and management and the judicious use of organizational resources. Centrally managed controls and processes may also meet independence requirements for assessments in support of initial and ongoing authorizations to operate and as part of organizational continuous monitoring.

Automated tools (e.g., security information and event management tools or enterprise security monitoring and management tools) can improve the accuracy, consistency, and availability of information associated with centrally managed controls and processes. Automation can also provide data aggregation and data correlation capabilities; alerting mechanisms; and dashboards to support risk-based decision-making within the organization.

As part of the control selection processes, organizations determine the controls that may be suitable for central management based on resources and capabilities. It is not always possible to centrally manage every aspect of a control. In such cases, the control can be treated as a hybrid control with the control managed and implemented centrally or at the system level. The controls and control enhancements that are candidates for full or partial central management include but are not limited to: AC-2(1), AC-2(2), AC-2(3), AC-2(4), AC-4(all), AC-17(1), AC-17(2), AC-

17(3), AC-17(9), AC-18(1), AC-18(3), AC-18(4), AC-18(5), AC-19(4), AC-22, AC-23, AT-2(1), AT-2(2), AT-3(1), AT-3(2), AT-3(3), AT-4, AU-3, AU-6(1), AU-6(3), AU-6(5), AU-6(6), AU-6(9), AU-7(1), AU-7(2), AU-11, AU-13, AU-16, CA-2(1), CA-2(2), CA-2(3), CA-3(1), CA-3(2), CA-3(3), CA-7(1), CA-9, CM-2(2), CM-3(1), CM-3(4), CM-4, CM-6, CM-6(1), CM-7(2), CM-7(4), CM-7(5), CM-8(all), CM-9(1), CM-10, CM-11, CP-7(all), CP-8(all), SC-43, SI-2, SI-3, SI-4(all), SI-7, SI-8.

Related Controls: PL-8.

PL-10 BASELINE SELECTION

[Priority 3]

Control:

Select a control baseline for the system.

Discussion: Control baselines are predefined sets of controls specifically assembled to address the protection needs of a group, organization, or community of interest. Controls are chosen for baselines to either satisfy mandates imposed by laws, executive orders, directives, regulations, policies, standards, and guidelines or address threats common to all users of the baseline under the assumptions specific to the baseline. Baselines represent a starting point for the protection of individuals' privacy, information, and information systems with subsequent tailoring actions to manage risk in accordance with mission, business, or other constraints (see PL-11). Federal control baselines are provided in [SP 800-53B]. The selection of a control baseline is determined by the needs of stakeholders. Stakeholder needs consider mission and business requirements as well as mandates imposed by applicable laws, executive orders, directives, policies, regulations, standards, and guidelines. For example, the control baselines in [SP 800-53B] are based on the requirements from [FISMA] and [PRIVACT]. The requirements, along with the NIST standards and guidelines implementing the legislation, direct organizations to select one of the control baselines after the reviewing the information types and the information that is processed, stored, and transmitted on the system; analyzing the potential adverse impact of the loss or compromise of the information or system on the organization's operations and assets, individuals, other organizations, or the Nation; and considering the results from system and organizational risk assessments. [CNSSI 1253] provides guidance on control baselines for national security systems.

Related Controls: PL-2, PL-11, RA-2, RA-3, SA-8.

PL-11 BASELINE TAILORING

[Priority 3]

Control:

Tailor the selected control baseline by applying specified tailoring actions.

Discussion: The concept of tailoring allows organizations to specialize or customize a set of baseline controls by applying a defined set of tailoring actions. Tailoring actions facilitate such specialization and customization by allowing organizations to develop security and privacy plans

that reflect their specific mission and business functions, the environments where their systems operate, the threats and vulnerabilities that can affect their systems, and any other conditions or situations that can impact their mission or business success. Tailoring guidance is provided in [SP 800-53B]. Tailoring a control baseline is accomplished by identifying and designating common controls, applying scoping considerations, selecting compensating controls, assigning values to control parameters, supplementing the control baseline with additional controls as needed, and providing information for control implementation. The general tailoring actions in [SP 800-53B] can be supplemented with additional actions based on the needs of organizations. Tailoring actions can be applied to the baselines in [SP 800-53B] in accordance with the security and privacy requirements from [FISMA], [PRIVACT], and [OMB A-130]. Alternatively, other communities of interest adopting different control baselines can apply the tailoring actions in [SP 800-53B] to specialize or customize the controls that represent the specific needs and concerns of those entities.

Related Controls: PL-10, RA-2, RA-3, RA-9, SA-8.

PERSONNEL SECURITY (PS)

Having proper security measures against the insider threat is a critical component for the CJIS Security Policy. This section's security terms and requirements apply to all personnel who have unescorted access to unencrypted CJI. Regardless of the implementation model – physical data center, virtual cloud solution, or a hybrid model – unescorted access to unencrypted CJI must be determined by the criminal and noncriminal justice agency taking into consideration if those individuals have unescorted logical or physical access to any information system resulting in the ability, right, or privilege to view, modify, or make use of unencrypted CJI.

PS-1 POLICY AND PROCEDURES

[Priority 2]

Control:

- a. Develop, document, and disseminate to organizational personnel with personnel security responsibilities:
 1. Agency-level personnel security policy that:
 - a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 - b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
 2. Procedures to facilitate the implementation of the personnel security policy and the associated personnel security controls;
- b. Designate organizational personnel with information security responsibilities to manage the development, documentation, and dissemination of the personnel security policy and procedures; and
- c. Review and update the current personnel security:
 1. Policy annually and following assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
 2. Procedures annually and following assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Discussion: Personnel security policy and procedures for the controls in the PS family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on their development. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission level or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies reflecting the complex nature of organizations. Procedures can be established for security and privacy programs, for

mission/business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents.

Events that may precipitate an update to personnel security policy and procedures include, but are not limited to, assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PS-8, SI-12.

PS-2 POSITION RISK DESIGNATION

[Priority 2]

Control:

- a. Assign a risk designation to all organizational positions;
- b. Establish screening criteria for individuals filling those positions; and
- c. Review and update position risk designations as required.

Discussion: Position risk designations reflect Office of Personnel Management (OPM) policy and guidance. Proper position designation is the foundation of an effective and consistent suitability and personnel security program. The Position Designation System (PDS) assesses the duties and responsibilities of a position to determine the degree of potential damage to the efficiency or integrity of the service due to misconduct of an incumbent of a position and establishes the risk level of that position. The PDS assessment also determines if the duties and responsibilities of the position present the potential for position incumbents to bring about a material adverse effect on national security and the degree of that potential effect, which establishes the sensitivity level of a position. The results of the assessment determine what level of investigation is conducted for a position. Risk designations can guide and inform the types of authorizations that individuals receive when accessing organizational information and information systems.

Position screening criteria include explicit information security role appointment requirements. Parts 1400 and 731 of Title 5, Code of Federal Regulations, establish the requirements for federal organizations to evaluate relevant covered positions for a position sensitivity and position risk designation commensurate with the duties and responsibilities of those positions.

Related Controls: AC-5, AT-3, PE-2, PE-3, PL-2, PS-3, PS-6, SA-5, SI-12.

PS-3 PERSONNEL SCREENING

[Existing] [Priority 2]

Control:

- a. Screen individuals prior to authorizing access to the information system;
 1. To properly screen, state of residency and national fingerprint-based record checks shall be conducted. National fingerprint-based record checks must be conducted pursuant to an FBI approved authority such as a federal statute or a state statute approved pursuant to Public Law 92-544. If the person resides in a different state than that of the assigned agency, the agency shall also conduct state (of the agency) record checks. When appropriate, the screening shall be consistent with:
 - a. 5 CFR 731.106; and/or
 - b. Office of Personnel Management policy, regulations, and guidance; and/or
 - c. agency policy, regulations, and guidance.

Agencies authorized to bypass state repositories in compliance with federal law must only conduct a national fingerprint-based record check.

Agencies without approved statutory authority authorizing or requiring civil fingerprint-based record checks on personnel with access to CHRI are exempt from this requirement until such time as appropriate statutory authority is obtained to conduct such record checks.

2. All requests for access shall be made as specified by the CSO, Authorized Recipient Official, or IA Official. The CSO/designee, Authorized Recipient Official/designee, or IA Official is authorized to approve access to CJI. All CSO designees shall be from an authorized criminal justice agency. All Authorized Recipient designees shall be employed by the Authorized Recipient Agency.
3. If a criminal history record of any kind exists, access to CJI shall not be granted until the CSO/designee, Authorized Recipient Official/designee, or IA Official reviews the matter to determine if access is appropriate.
 - a. If a felony conviction of any kind exists, the agency shall deny access to CJI. However, the requesting agency may ask for a review by the CSO/designee, Authorized Recipient Official/designee, or IA Official in extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance.
 - b. Applicants with a record of misdemeanor offense(s) may be granted access if the CSO/designee, Authorized Recipient Official/designee, or IA Official, determines the nature or severity of the misdemeanor offense(s) do not warrant disqualification. The requesting agency may request the CSO/designee, Authorized Recipient Official/designee, or IA Official review a denial of access determination.
 - c. If a criminal history record of any kind is found on a contractor, the CA shall be formally notified of continuing fitness determination and system access shall be delayed pending review of the criminal history record information. The CA shall in turn notify the contractor's security officer.
4. If the person appears to be a fugitive or has an arrest history without conviction, the CSO/designee, Authorized Recipient Official/designee, or IA Official shall review the

matter to determine if access to CJI is appropriate.

5. If the person already has access to CJI and is subsequently arrested and or convicted, continued access to CJI shall be determined by the CSO/designee, Authorized Recipient Official/designee, or IA Official. This does not implicitly grant hiring/firing authority with the CSA, Authorized Recipient, or IA Official only the authority to grant access to CJI. For offenses other than felonies, the CSO/designee, Authorized Recipient Official/designee, or IA Official has the latitude to delegate continued access determinations.
6. If the CSO/designee, Authorized Recipient Official/designee, or IA Official determines that access to CJI by the person would not be in the public interest, access shall be denied and the person's appointing authority shall be notified in writing of the access denial.
7. The criminal and non-criminal justice agency shall maintain a list of personnel who have been authorized unescorted access to unencrypted CJI and shall, upon request, provide a current copy of the access list to the CSO/designee, Authorized Recipient Official/designee, or IA Official.

and

- b. Recommend rescreening individuals in accordance with PS-3(a)(1) above. The authority authorized for the national fingerprint-based background check must also authorize the rescreening.

Discussion: Personnel screening and rescreening activities reflect applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and specific criteria established for the risk designations of assigned positions. Examples of personnel screening include background investigations and agency checks.

Organizations may define different rescreening conditions and frequencies for personnel accessing systems based on types of information processed, stored, or transmitted by the systems.

Related Controls: AC-2, IA-4, MA-5, PE-2, PS-2, PS-6, PS-7.

PS-4 PERSONNEL TERMINATION

[Priority 2]

Control:

Upon termination of individual employment:

- a. Disable system access within twenty-four (24) hours;
- b. Terminate or revoke any authenticators and credentials associated with the individual;
- c. Conduct exit interviews that include a discussion of non-disclosure of CJI and PII;
- d. Retrieve all security-related organizational system-related property; and
- e. Retain access to organizational information and systems formerly controlled by

terminated individual.

Discussion: System property includes hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes. Exit interviews ensure that terminated individuals understand the security constraints imposed by being former employees and that proper accountability is achieved for system-related property. Security topics at exit interviews include reminding individuals of nondisclosure agreements and potential limitations on future employment. Exit interviews may not always be possible for some individuals, including in cases related to the unavailability of supervisors, illnesses, or job abandonment. Exit interviews are important for individuals with security clearances. The timely execution of termination actions is essential for individuals who have been terminated for cause. In certain situations, organizations consider disabling the system accounts of individuals who are being terminated prior to the individuals being notified.

Related Controls: AC-2, IA-4, PE-2, PS-6, PS-7.

PS-5 PERSONNEL TRANSFER

[Priority 3]

Control:

- a. Review and confirm ongoing operational need for current logical and physical access authorizations to systems and facilities when individuals are reassigned or transferred to other positions within the organization;
- b. Initiate appropriate actions such as closing and establishing accounts and changing system access authorizations within twenty-four (24) hours;
- c. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and
- d. Notify organizational personnel with information security responsibilities, organizational personnel with personnel security responsibilities, system/network administrators, and organizational personnel with account management responsibilities prior to personnel transfer.

Discussion: Personnel transfer applies when reassignments or transfers of individuals are permanent or of such extended duration as to make the actions warranted.

Organizations define actions appropriate for the types of reassignments or transfers, whether permanent or extended. Actions that may be required for personnel transfers or reassignments to other positions within organizations include returning old and issuing new keys, identification cards, and building passes; closing system accounts and establishing new accounts; changing system access authorizations (i.e., privileges); and providing for access to official records to which individuals had access at previous work locations and in previous system accounts.

Related Controls: AC-2, IA-4, PE-2, PS-4, PS-7.

PS-6 ACCESS AGREEMENTS

[Priority 4]

Control:

- a. Develop and document access agreements for organizational systems;
- b. Review and update the access agreements at least annually; and
- c. Verify that individuals requiring access to organizational information and systems:
 1. Sign appropriate access agreements prior to being granted access; and
 2. Re-sign access agreements to maintain access to organizational systems when access agreements have been updated or when signatories change.

Discussion: Access agreements include nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with organizational systems to which access is authorized. Organizations can use electronic signatures to acknowledge access agreements unless specifically prohibited by organizational policy.

Related Controls: AC-17, PE-2, PL-4, PS-2, PS-3, PS-6, PS-7, PS-8, SI-12.

PS-7 EXTERNAL PERSONNEL SECURITY

[Existing] [Priority 2]

Control:

- a. Establish personnel security requirements, including security roles and responsibilities for external providers;
- b. Require external providers to comply with personnel security policies and procedures established by the organization;
- c. Document personnel security requirements;
- d. Require external providers to notify organizational personnel with information security responsibilities, organizational personnel with personnel security responsibilities, system/network administrators, or organizational personnel with account management responsibilities of any personnel transfers or terminations of external personnel who possess organizational credentials and/or badges, or who have system privileges within twenty-four (24) hours; and
- e. Monitor provider compliance with personnel security requirements.

Discussion: External provider refers to organizations other than the organization operating or acquiring the system. External providers include service bureaus, contractors, and other organizations that provide system development, information technology services, testing or assessment services, outsourced applications, and network/security management. Organizations explicitly include personnel security requirements in acquisition-related documents. External providers may have personnel working at organizational facilities with credentials, badges, or

system privileges issued by organizations. Notifications of external personnel changes ensure the appropriate termination of privileges and credentials. Organizations define the transfers and terminations deemed reportable by security-related characteristics that include functions, roles, and the nature of credentials or privileges associated with transferred or terminated individuals.

Related Controls: AT-2, AT-3, MA-5, PE-3, PS-2, PS-3, PS-4, PS-5, PS-6, SA-5, SA- 9.

PS-8 PERSONNEL SANCTIONS

[Priority 4]

Control:

- a. Employ a formal sanctions process for individuals failing to comply with established information security and privacy policies and procedures; and
- b. Notify organizational personnel with information security responsibilities, organizational personnel with personnel security responsibilities, system/network administrators, or organizational personnel with account management responsibilities within twenty-four (24) hours when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

Discussion: Organizational sanctions reflect applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Sanctions processes are described in access agreements and can be included as part of general personnel policies for organizations and/or specified in security and privacy policies.

Organizations consult with the Office of the General Counsel regarding matters of employee sanctions.

Related Controls: All XX-1 Controls, PL-4, PS-6.

PS-9 POSITION DESCRIPTIONS

[Priority 4]

Control:

Incorporate security and privacy roles and responsibilities into organizational position descriptions.

Discussion: Specification of security and privacy roles in individual organizational position descriptions facilitates clarity in understanding the security or privacy responsibilities associated with the roles and the role-based security and privacy training requirements for the roles.

Figure 13 – Personnel Security Use Cases

Use Case 1 – A Local Police Department’s Personnel Security Controls

A local police department implemented a replacement CAD system that integrated to their state’s CSA and was authorized to process CJI. In addition to the physical and technical controls already in place, the police department implemented a variety of personnel security controls to reduce the insider threat. The police department used background screening consistent with the FBI CJIS Security Policy to vet those with unescorted access to areas in which CJI is processed, including the IT administrators employed by a contractor and all janitorial staff. The police department established sanctions against any vetted person found to be in violation of stated policies. The police department re-evaluated each person’s suitability for access to CJI every five years.

Use Case 2 – Infrastructure as a Service (IaaS) Cloud Service Implementation

This model provides the consumer the capability to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, including operating systems and applications.

When using the IaaS service model the consumer may have control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls), but does not manage or control the underlying cloud infrastructure – as defined in Appendix G.3.

A local agency implements an IaaS solution in a cloud environment leveraging an agency-implemented secure virtual private cloud which has been identified to meet the appropriate security controls in the CJIS Security Policy. The agency maintains sole access to the encryption keys. In this scenario, cloud service provider personnel have no logical or physical access to any information system resulting in the ability, right, or privilege to view, modify, or make use of unencrypted CJI; therefore, no fingerprint-based background checks are required to comply with the CJIS Security Policy. Refer to Appendix G.3 Cloud Computing for additional implementation guidance.

Use Case 3 – Platform as a Service (PaaS) Cloud Service Implementation

This model provides the consumer the capability to deploy consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider onto the cloud infrastructure.*

** This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources.*

When using the PaaS service model, the consumer may have control over the deployed applications and possibly configuration settings for the application-hosting environment, but does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage – as defined in Appendix G.3.

An agency utilizes a cloud service solution involving PaaS to write code, build, or develop a new application. There is no CJI associated with the code development. Although cloud service personnel provide support for the platform (i.e., hardware and software maintenance), no CJI is being accessed during development. The cloud service provider has no unescorted logical or physical access to any information system and no ability, right, or privilege to view, modify, or make use of unencrypted CJI. Refer to Appendix G.3 Cloud Computing for additional implementation guidance.

Use Case 4 – Software as a Service (SaaS) Cloud Service Implementation

The SaaS service model is often referred to as “Software deployed as a hosted service and accessed over the Internet.”

The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface.

When using the SaaS service model, it should be understood that the consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings – as defined in Appendix G.3

An agency utilizes a SaaS provider for their records management system (RMS). The SaaS provider hosts their solution on a cloud provider. The SaaS provider directly supports the agency for updates and management of the solution and has unescorted logical or physical access to the information system resulting in the ability, right, or privilege to view, modify, or make use of unencrypted CJI within the RMS. The cloud provider, however, does not have unescorted logical or physical access to any information system resulting in the ability, right, or privilege to view, modify, or make use of unencrypted CJI as the SaaS provider maintains the encryption keys. In this scenario, the agency would be required to comply with Section 5.12 for employees of the SaaS provider with access to CJI but would not need to do so for employees of the cloud provider used by the SaaS provider. Refer to Appendix G.3 Cloud Computing for additional implementation guidance.

RISK ASSESSMENT (RA)

RA-1 POLICY AND PROCEDURES

[Priority 2]

Control:

- a. Develop, document, and disseminate to organizational personnel with risk assessment responsibilities:
 1. Agency Level risk assessment policy that:
 - (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 - (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
 2. Procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls;
- b. Designate organizational personnel with security and privacy responsibilities to manage the development, documentation, and dissemination of the risk assessment policy and procedures; and
- c. Review and update the current risk assessment:
 1. Policy annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI; and
 2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.

Discussion: Risk assessment policy and procedures address the controls in the RA family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of risk assessment policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies reflecting the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to risk assessment policy and procedures include assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PS-8, SI-12.

RA-2 SECURITY CATEGORIZATION

[Priority 2]

Control:

- a. Categorize the system and information it processes, stores, and transmits;
- b. Document the security categorization results, including supporting rationale, in the security plan for the system; and
- c. Verify that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.

Discussion: Security categories describe the potential adverse impacts or negative consequences to organizational operations, organizational assets, and individuals if organizational information and systems are compromised through a loss of confidentiality, integrity, or availability. Security categorization is also a type of asset loss characterization in systems security engineering processes that is carried out throughout the system development life cycle. Organizations can use privacy risk assessments or privacy impact assessments to better understand the potential adverse effects on individuals. The FBI CJIS Advisory Policy Board (APB) has assigned a security categorization of “moderate” for CJI and systems that process, store, and transmit CJI.

Organizations conduct the security categorization process as an organization-wide activity with the direct involvement of chief information officers, senior agency information security officers, senior agency officials for privacy, system owners, mission and business owners, and information owners or stewards.

Security categorization processes facilitate the development of inventories of information assets and, along with CM-8, mappings to specific system components where information is processed, stored, or transmitted. The security categorization process is revisited throughout the system development life cycle to ensure that the security categories remain accurate and relevant.

Related Controls: CM-8, MP-4, PL-2, PL-10, PL-11, RA-3, RA-5, RA-7, SA-8, SC-7, SI-12.

RA-3 RISK ASSESSMENT

[Priority 2]

Control:

- a. Conduct a risk assessment, including:
 1. Identifying threats to and vulnerabilities in the system;
 2. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and
 3. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information;
- b. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments;

- c. Document risk assessment results in a risk assessment report;
- d. Review risk assessment results at least quarterly;
- e. Disseminate risk assessment results to organizational personnel with risk assessment responsibilities and organizational personnel with security and privacy responsibilities; and
- f. Update the risk assessment at least quarterly or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.

Discussion: Risk assessments consider threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals, other organizations, and the Nation. Risk assessments also consider risk from external parties, including contractors who operate systems on behalf of the organization, individuals who access organizational systems, service providers, and outsourcing entities.

Organizations can conduct risk assessments at all three levels in the risk management hierarchy (i.e., organization level, mission/business process level, or information system level) and at any stage in the system development life cycle. Risk assessments can also be conducted at various steps in the Risk Management Framework, including preparation, categorization, control selection, control implementation, control assessment, authorization, and control monitoring. Risk assessment is an ongoing activity carried out throughout the system development life cycle.

Risk assessments can also address information related to the system, including system design, the intended use of the system, testing results, and supply chain-related information or artifacts. Risk assessments can play an important role in control selection processes, particularly during the application of tailoring guidance and in the earliest phases of capability determination.

Related Controls: CA-3, CA-6, CM-4, CP-6, CP-7, IA-8, MA-5, PE-3, PE-8, PL-2, PL-10, PL-11, RA-2, RA-5, RA-7, SA-8, SA-9, SI-12.

RA-5 VULNERABILITY MONITORING AND SCANNING

[Priority 1]

Control:

- a. Monitor and scan for vulnerabilities in the system and hosted applications at least monthly and when new vulnerabilities potentially affecting the system are identified and reported;
- b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
 - 1. Enumerating platforms, software flaws, and improper configurations;
 - 2. Formatting checklists and test procedures; and
 - 3. Measuring vulnerability impact;
- c. Analyze vulnerability scan reports and results from vulnerability monitoring;
- d. Remediate legitimate vulnerabilities within the number of days listed;
 - Critical—15 days

- High—30 days
 - Medium—60 days
 - Low—90 days; and
- e. Share information obtained from the vulnerability monitoring process and control assessments with organizational personnel with risk assessment, control assessment, and vulnerability scanning responsibilities to help eliminate similar vulnerabilities in other systems; and
 - f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.

Discussion: Security categorization of information and systems guides the frequency and comprehensiveness of vulnerability monitoring (including scans). Organizations determine the required vulnerability monitoring for system components, ensuring that the potential sources of vulnerabilities—such as infrastructure components (e.g., switches, routers, guards, sensors), networked printers, scanners, and copiers—are not overlooked. The capability to readily update vulnerability monitoring tools as new vulnerabilities are discovered and announced and as new scanning methods are developed helps to ensure that new vulnerabilities are not missed by employed vulnerability monitoring tools. The vulnerability monitoring tool update process helps to ensure that potential vulnerabilities in the system are identified and addressed as quickly as possible. Vulnerability monitoring and analyses for custom software may require additional approaches, such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Organizations can use these analysis approaches in source code reviews and in a variety of tools, including web-based application scanners, static analysis tools, and binary analyzers.

Vulnerability monitoring includes scanning for patch levels; scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and scanning for flow control mechanisms that are improperly configured or operating incorrectly. Vulnerability monitoring may also include continuous vulnerability monitoring tools that use instrumentation to continuously analyze components. Instrumentation-based tools may improve accuracy and may be run throughout an organization without scanning. Vulnerability monitoring tools that facilitate interoperability include tools that are Security Content Automated Protocol (SCAP)-validated. Thus, organizations consider using scanning tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that employ the Open Vulnerability Assessment Language (OVAL) to determine the presence of vulnerabilities. Sources for vulnerability information include the Common Weakness Enumeration (CWE) listing and the National Vulnerability Database (NVD). Control assessments, such as red team exercises, provide additional sources of potential vulnerabilities for which to scan. Organizations also consider using scanning tools that express vulnerability impact by the Common Vulnerability Scoring System (CVSS).

Vulnerability monitoring includes a channel and process for receiving reports of security vulnerabilities from the public at-large. Vulnerability disclosure programs can be as simple as publishing a monitored email address or web form that can receive reports, including notification authorizing good-faith research and disclosure of security vulnerabilities. Organizations generally expect that such research is happening with or without their authorization and can use

public vulnerability disclosure channels to increase the likelihood that discovered vulnerabilities are reported directly to the organization for remediation.

Organizations may also employ the use of financial incentives (also known as “bug bounties”) to further encourage external security researchers to report discovered vulnerabilities. Bug bounty programs can be tailored to the organization’s needs. Bounties can be operated indefinitely or over a defined period of time and can be offered to the general public or to a curated group. Organizations may run public and private bounties simultaneously and could choose to offer partially credentialed access to certain participants in order to evaluate security vulnerabilities from privileged vantage points.

Related Controls: CA-2, CA-7, CM-2, CM-4, CM-6, CM-8, RA-2, RA-3, SA-11, SA-15, SI-2, SI-3, SI-4, SI-7, SR-11.

Control Enhancements:

(2) VULNERABILITY MONITORING AND SCANNING | UPDATE VULNERABILITIES TO BE SCANNED

[Priority 1]

Control:

Update the system vulnerabilities to be scanned within 24 hours prior to running a new scan or when new vulnerabilities are identified and reported.

Discussion: Due to the complexity of modern software, systems, and other factors, new vulnerabilities are discovered on a regular basis. It is important that newly discovered vulnerabilities are added to the list of vulnerabilities to be scanned to ensure that the organization can take steps to mitigate those vulnerabilities in a timely manner.

Related Controls: SI-5.

(5) VULNERABILITY MONITORING AND SCANNING | PRIVILEGED ACCESS

[Priority 1]

Control:

Implement privileged access authorization to information system components containing or processing CJI for vulnerability scanning activities requiring privileged access.

Discussion: In certain situations, the nature of the vulnerability scanning may be more intrusive, or the system component that is the subject of the scanning may contain classified or controlled unclassified information, such as personally identifiable information. Privileged access authorization to selected system components facilitates more thorough vulnerability scanning and protects the sensitive nature of such scanning.

Related Controls: None.

(11) VULNERABILITY MONITORING AND SCANNING | PUBLIC DISCLOSURE PROGRAM

[Priority 1]

Control:

Establish a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components.

Discussion: The reporting channel is publicly discoverable and contains clear language authorizing good-faith research and the disclosure of vulnerabilities to the organization. The organization does not condition its authorization on an expectation of indefinite non-disclosure to the public by the reporting entity but may request a specific time period to properly remediate the vulnerability.

Related Controls: None.

RA-7 RISK RESPONSE

[Priority 2]

Control:

Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.

Discussion: Organizations have many options for responding to risk including mitigating risk by implementing new controls or strengthening existing controls, accepting risk with appropriate justification or rationale, sharing or transferring risk, or avoiding risk. The risk tolerance of the organization influences risk response decisions and actions. Risk response addresses the need to determine an appropriate response to risk before generating a plan of action and milestones entry. For example, the response may be to accept risk or reject risk, or it may be possible to mitigate the risk immediately so that a plan of action and milestones entry is not needed.

However, if the risk response is to mitigate the risk, and the mitigation cannot be completed immediately, a plan of action and milestones entry is generated.

Related Controls: CA-5, RA-2, RA-3, SR-2.

RA-9 CRITICALITY ANALYSIS

[Priority 2]

Control:

Identify critical system components and functions by performing a criticality analysis for information system components containing or processing CJI at the planning, design, development, testing, implementation, and maintenance stages of the system development life cycle.

Discussion: Not all system components, functions, or services necessarily require significant protections. For example, criticality analysis is a key tenet of supply chain risk management and informs the prioritization of protection activities. The identification of critical system components and functions considers applicable laws, executive orders, regulations, directives, policies, standards, system functionality requirements, system and component interfaces, and system and component dependencies. Systems engineers conduct a functional decomposition of

a system to identify mission-critical functions and components. The functional decomposition includes the identification of organizational missions supported by the system, decomposition into the specific functions to perform those missions, and traceability to the hardware, software, and firmware components that implement those functions, including when the functions are shared by many components within and external to the system.

The operational environment of a system or a system component may impact the criticality, including the connections to and dependencies on cyber-physical systems, devices, system-of-systems, and outsourced IT services. System components that allow unmediated access to critical system components or functions are considered critical due to the inherent vulnerabilities that such components create. Component and function criticality are assessed in terms of the impact of a component or function failure on the organizational missions that are supported by the system that contains the components and functions.

Criticality analysis is performed when an architecture or design is being developed, modified, or upgraded. If such analysis is performed early in the system development life cycle, organizations may be able to modify the system design to reduce the critical nature of these components and functions, such as by adding redundancy or alternate paths into the system design. Criticality analysis can also influence the protection measures required by development contractors. In addition to criticality analysis for systems, system components, and system services, criticality analysis of information is an important consideration. Such analysis is conducted as part of security categorization in RA-2.

Related Controls: CP-2, PL-2, PL-8, PL-11, RA-2, SA-8, SA-15, SR-5.

SYSTEM AND SERVICES ACQUISITION (SA)

SA-1 POLICY AND PROCEDURES

[Priority 2]

Control:

- a. Develop, document, and disseminate to: organizational personnel with system and services acquisition responsibilities; organizational personnel with information security and privacy responsibilities; organizational personnel with supply chain risk management responsibilities:
 1. Agency/Entity information systems and services acquisition policy for systems used to process, store, or transmit CJI that:
 - (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 - (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
 2. Procedures to facilitate the implementation of the system and services acquisition policy and the associated system and services acquisition controls;
- b. Designate organizational personnel with information security responsibilities and organizational personnel with system and services acquisition responsibilities to manage the development, documentation, and dissemination of the system and services acquisition policy and procedures; and
- c. Review and update the current system and services acquisition:
 1. Policy following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI; and
 2. Procedures following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.

Discussion: System and services acquisition policy and procedures address the controls in the SA family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of system and services acquisition policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events

that may precipitate an update to system and services acquisition policy and procedures include assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PS-8, SA-8, SI-12.

SA-2 ALLOCATION OF RESOURCES

[Priority 2]

Control:

- a. Determine the high-level information security and privacy requirements for the system or system service in mission and business process planning;
- b. Determine, document, and allocate the resources required to protect the system or system service as part of the organizational capital planning and investment control process; and

Discussion: Resource allocation for information security and privacy includes funding for system and services acquisition, sustainment, and supply chain-related risks throughout the system development life cycle.

Related Controls: SA-9, SR-3, SR-5.

SA-3 SYSTEM DEVELOPMENT LIFE CYCLE

[Priority 2]

Control:

- a. Acquire, develop, and manage the system using an agency documented system development lifecycle process that incorporates information security and privacy considerations;
- b. Define and document information security and privacy roles and responsibilities throughout the system development life cycle;
- c. Identify individuals having information security and privacy roles and responsibilities; and
- d. Integrate the organizational information security and privacy risk management process into system development life cycle activities.

Discussion: A system development life cycle process provides the foundation for the successful development, implementation, and operation of organizational systems. The integration of security and privacy considerations early in the system development life cycle is a foundational principle of systems security engineering and privacy engineering. To apply the required controls within the system development life cycle requires a basic understanding of

information security and privacy, threats, vulnerabilities, adverse impacts, and risk to critical mission and business functions. The security engineering principles in SA-8 help individuals properly design, code, and test systems and system components. Organizations include qualified personnel (e.g., senior agency information security officers, senior agency officials for privacy, security and privacy architects, and security and privacy engineers) in system development life cycle processes to ensure that established security and privacy requirements are incorporated into organizational systems. Role-based security and privacy training programs can ensure that individuals with key security and privacy roles and responsibilities have the experience, skills, and expertise to conduct assigned system development life cycle activities.

The effective integration of security and privacy requirements into enterprise architecture also helps to ensure that important security and privacy considerations are addressed throughout the system life cycle and that those considerations are directly related to organizational mission and business processes. This process also facilitates the integration of the information security and privacy architectures into the enterprise architecture, consistent with the risk management strategy of the organization. Because the system development life cycle involves multiple organizations (e.g., external suppliers, developers, integrators, service providers), acquisition and supply chain risk management functions and controls play significant roles in the effective management of the system during the life cycle.

Related Controls: PL-8, SA-4, SA-5, SA-8, SA-11, SA-15, SA-22, SR-3, SR-5,

SA-4 ACQUISITION PROCESS

[Priority 2]

Control:

Include the following requirements, descriptions, and criteria, explicitly or by reference, using agency defined contract language in the acquisition contract for the system, system component, or system service:

- a. Security and privacy functional requirements;
- b. Strength of mechanism requirements;
- c. Security and privacy assurance requirements;
- d. Controls needed to satisfy the security and privacy requirements.
- e. Security and privacy documentation requirements;
- f. Requirements for protecting security and privacy documentation;
- g. Description of the system development environment and environment in which the system is intended to operate;
- h. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; and
- i. Acceptance criteria.

Discussion: Security and privacy functional requirements are typically derived from the high-level security and privacy requirements described in SA-2. The derived requirements include security and privacy capabilities, functions, and mechanisms. Strength requirements associated with such capabilities, functions, and mechanisms include degree of correctness, completeness, resistance to tampering or bypass, and resistance to direct attack. Assurance requirements include development processes, procedures, and methodologies as well as the evidence from development and assessment activities that provide grounds for confidence that the required functionality is implemented and possesses the required strength of mechanism.

Controls can be viewed as descriptions of the safeguards and protection capabilities appropriate for achieving the particular security and privacy objectives of the organization and for reflecting the security and privacy requirements of stakeholders. Controls are selected and implemented in order to satisfy system requirements and include developer and organizational responsibilities.

Controls can include technical, administrative, and physical aspects. In some cases, the selection and implementation of a control may necessitate additional specification by the organization in the form of derived requirements or instantiated control parameter values. The derived requirements and control parameter values may be necessary to provide the appropriate level of implementation detail for controls within the system development life cycle.

Security and privacy documentation requirements address all stages of the system development life cycle. Documentation provides user and administrator guidance for the implementation and operation of controls. The level of detail required in such documentation is based on the security categorization or classification level of the system and the degree to which organizations depend on the capabilities, functions, or mechanisms to meet risk response expectations. Requirements can include mandated configuration settings that specify allowed functions, ports, protocols, and services. Acceptance criteria for systems, system components, and system services are defined in the same manner as the criteria for any organizational acquisition or procurement.

Related Controls: CM-6, CM-8, PS-7, SA-3, SA-5, SA-8, SA-11, SA-15, SR-3, SR-5.

Control Enhancements:

(1) ACQUISITION PROCESS | FUNCTIONAL PROPERTIES OF CONTROLS

[Priority 2]

Control:

Require the developer of the system, system component, or system service to provide a description of the functional properties of the controls to be implemented.

Discussion: Functional properties of security and privacy controls describe the functionality (i.e., security or privacy capability, functions, or mechanisms) visible at the interfaces of the controls and specifically exclude functionality and data structures internal to the operation of the controls.

Related Controls: None.

(2) ACQUISITION PROCESS | DESIGN AND IMPLEMENTATION INFORMATION FOR CONTROLS

[Priority 2]

Control:

Require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes: security-relevant external system interfaces; high-level design and a project plan that addresses sufficient detail to permit analysis and testing of the controls.

Discussion: Organizations may require different levels of detail in the documentation for the design and implementation of controls in organizational systems, system components, or system services based on mission and business requirements, requirements for resiliency and trustworthiness, and requirements for analysis and testing. Systems can be partitioned into multiple subsystems. Each subsystem within the system can contain one or more modules. The high-level design for the system is expressed in terms of subsystems and the interfaces between subsystems providing security-relevant functionality. The low-level design for the system is expressed in terms of modules and the interfaces between modules providing security-relevant functionality. Design and implementation documentation can include manufacturer, version, serial number, verification hash signature, software libraries used, date of purchase or download, and the vendor or download source. Source code and hardware schematics are referred to as the implementation representation of the system.

Related Controls: None.

(9) ACQUISITION PROCESS | FUNCTIONS, PORTS, PROTOCOLS, AND SERVICES IN USE

[Priority 2]

Control:

Require the developer of the system, system component, or system service to identify the functions, ports, protocols, and services intended for organizational use.

Discussion: The identification of functions, ports, protocols, and services early in the system development life cycle (e.g., during the initial requirements definition and design stages) allows organizations to influence the design of the system, system component, or system service. This early involvement in the system development life cycle helps organizations avoid or minimize the use of functions, ports, protocols, or services that pose unnecessarily high risks and understand the trade-offs involved in blocking specific ports, protocols, or services or requiring

system service providers to do so. Early identification of functions, ports, protocols, and services avoids costly retrofitting of controls after the system, component, or system service has been implemented. SA-9 describes the requirements for external system services. Organizations identify which functions, ports, protocols, and services are provided from external sources.

Related Controls: CM-7, SA-9.

(10) ACQUISITION PROCESS | USE OF APPROVED PIV PRODUCTS

[Priority 2]

Control:

Employ only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational systems.

Discussion: Products on the FIPS 201-approved products list meet requirements for Personal Identity Verification (PIV) of Federal Employees and Contractors. PIV cards are used for multi-factor authentication in systems and organizations.

Related Controls: IA-2, IA-8.

SA-5 SYSTEM DOCUMENTATION

[Priority 3]

Control:

- a. Obtain or develop administrator documentation for the system, system component, or system service that describes:
 1. Secure configuration, installation, and operation of the system, component, or service;
 2. Effective use and maintenance of security and privacy functions and mechanisms; and
 3. Known vulnerabilities regarding configuration and use of administrative or privileged functions;
- b. Obtain or develop user documentation for the system, system component, or system service that describes:
 1. User-accessible security and privacy functions and mechanisms and how to effectively use those functions and mechanisms;
 2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner and protect individual privacy; and
 3. User responsibilities in maintaining the security of the system, component, or service and privacy of individuals;

- c. Document steps to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent by contacting manufacturers, suppliers, or developers and conducting web-based searches in response; and
- d. Distribute documentation to organizational personnel with system and services responsibilities.

Discussion: System documentation helps personnel understand the implementation and operation of controls. Organizations consider establishing specific measures to determine the quality and completeness of the content provided. System documentation may be used to support the management of supply chain risk, incident response, and other functions. Personnel or roles that require documentation include system owners, system security officers, and system administrators. Attempts to obtain documentation include contacting manufacturers or suppliers and conducting web-based searches. The inability to obtain documentation may occur due to the age of the system or component or the lack of support from developers and contractors. When documentation cannot be obtained, organizations may need to recreate the documentation if it is essential to the implementation or operation of the controls. The protection provided for the documentation is commensurate with the security category or classification of the system.

Documentation that addresses system vulnerabilities may require an increased level of protection. Secure operation of the system includes initially starting the system and resuming secure system operation after a lapse in system operation.

Related Controls: CM-4, CM-6, CM-7, CM-8, PL-2, PL-4, PL-8, PS-2, SA-3, SA-4, SA-8, SA-9, SA-10, SA-11, SA-15, SI-12, SR-3.

SA-8 SECURITY AND PRIVACY ENGINEERING PRINCIPLES

[Priority 2]

Control:

Apply agency documented systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components.

Discussion: Systems security and privacy engineering principles are closely related to and implemented throughout the system development life cycle (see SA-3). Organizations can apply systems security and privacy engineering principles to new systems under development or to systems undergoing upgrades. For existing systems, organizations apply systems security and privacy engineering principles to system upgrades and modifications to the extent feasible, given the current state of hardware, software, and firmware components within those systems.

The application of systems security and privacy engineering principles helps organizations develop trustworthy, secure, and resilient systems and reduces the susceptibility to disruptions, hazards, threats, and the creation of privacy problems for individuals. Examples of system

security engineering principles include: developing layered protections; establishing security and privacy policies, architecture, and controls as the foundation for design and development; incorporating security and privacy requirements into the system development life cycle; delineating physical and logical security boundaries; ensuring that developers are trained on how to build secure software; tailoring controls to meet organizational needs; and performing threat modeling to identify use cases, threat agents, attack vectors and patterns, design patterns, and compensating controls needed to mitigate risk.

Organizations that apply systems security and privacy engineering concepts and principles can facilitate the development of trustworthy, secure systems, system components, and system services; reduce risk to acceptable levels; and make informed risk management decisions.

System security engineering principles can also be used to protect against certain supply chain risks, including incorporating tamper-resistant hardware into a design.

Related Controls: PL-8, RA-2, RA-3, RA-9, SA-3, SA-4, SA-15, SC-2, SC-39, SR-2, SR-3, SR- 5.

Control Enhancements:

(33) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | MINIMIZATION

[Priority 2]

Control:

Implement the privacy principle of minimization using only the Personally Identifiable Information necessary to perform system engineering.

Discussion: The principle of minimization states that organizations should only process personally identifiable information that is directly relevant and necessary to accomplish an authorized purpose and should only maintain personally identifiable information for as long as is necessary to accomplish the purpose. Organizations have processes in place, consistent with applicable laws and policies, to implement the principle of minimization.

Related Controls: PE-8, SI-12.

SA-9 EXTERNAL SYSTEM SERVICES

[Priority 2]

Control:

- a. Require that providers of external system services comply with organizational security and privacy requirements and employ system and services acquisition security controls in accordance with the CJISSECPOL including the following agreements when applicable:
 1. Management control agreement: A NCJA (government) designated to perform criminal justice functions for a CJA shall be eligible for access to the CJI. Access shall be permitted when such designation is authorized pursuant to executive order, statute, regulation, or interagency agreement. The NCJA shall sign and execute a management control agreement (MCA) with the CJA stipulating management control of the criminal justice function remains solely with the CJA. An example of an NCJA (government) is a city information technology (IT) department. An example of an MCA is provided in Appendix D.2.
 2. Security Addendum: The CJIS Security Addendum is a uniform addendum to an agreement between the government agency and a private contractor, approved by the Director of the FBI, acting for the U.S. Attorney General, as referenced in Title 28 CFR 20.33 (a)(7), which specifically authorizes access to CHRI, limits the use of the information to the purposes for which it is provided, ensures the security and confidentiality of the information is consistent with existing regulations and the CJISSECPOL, provides for sanctions, and contains such other provisions as the Attorney General may require.

Private contractors designated to:

- a. Perform criminal justice functions for a CJA; or
- b. Perform criminal justice dispatching functions or data processing/information services for a NCJA (government), shall be eligible for access to CJI pursuant to an agreement which specifically identifies the private contractor's purpose and scope of providing services for the administration of criminal justice. The agreement between the CJA/NCJA and the private contractor shall incorporate the CJISSECPOL.

Private contractors who perform criminal justice functions shall meet the same training and certification criteria required by governmental agencies performing a similar function and shall be subject to the same extent of audit review as are local user agencies. All private contractors who perform criminal justice functions shall acknowledge, via signing of the CJIS Security Addendum Certification page (page H- 8), compliance with all aspects of the CJIS Security Addendum. The CJIS Security Addendum is presented in Appendix H (pages H-6 and 7). Modifications to the CJIS Security Addendum shall be enacted only by the FBI.

3. Outsourcing Standards for Channelers: Channelers designated to request civil fingerprint-based background checks on behalf of a NCJA (public) or NCJA (private) for noncriminal justice functions shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. All Channelers accessing CJI shall be subject to the terms and conditions described in the Compact Council Security and

Management Control Outsourcing Standard. Each Channeler that directly accesses CJI shall also allow the FBI to conduct periodic penetration testing. Channelers leveraging CJI to perform civil functions on behalf of an Authorized Recipient shall meet the same training and certification criteria required by governmental agencies performing a similar function and shall be subject to the same extent of audit review as are local user agencies.

4. Outsourcing Standards for Non-Channelers: Contractors designated to perform noncriminal justice ancillary functions on behalf of a NCJA (public) or NCJA (private) for noncriminal justice functions shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. All contractors accessing CJI shall be subject to the terms and conditions described in the Compact Council Outsourcing Standard for Non-Channelers. Contractors leveraging CJI to perform civil functions on behalf of an Authorized Recipient shall meet the same training and certification criteria required by governmental agencies performing a similar function and shall be subject to the same extent of audit review as are local user agencies.
- b. Define and document organizational oversight and user roles and responsibilities with regard to external system services; and
 - c. Employ the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis:
 1. All agencies having access to CJI shall permit an inspection team to conduct an appropriate inquiry and audit of any alleged security violations.
 2. At a minimum, triennially audit all external service providers which have access to the information system in order to ensure compliance with applicable statutes, regulations, and policies.
 3. Have the authority to conduct unannounced security inspections and scheduled audits of external service providers facilities.
 4. Have the authority, on behalf of another CSA, to conduct a CJISSECPOL compliance audit of contractor facilities and provide the results to the requesting CSA. If a subsequent CSA requests an audit of the same contractor facility, the CSA may provide the results of the previous audit unless otherwise notified by the requesting CSA that a new audit be performed.

Note: Compliance audit requirements are outlined in the Security and Management Control Outsourcing Standard for Non-Channeler and Channeling related to outsourcing noncriminal justice administrative functions.

Discussion: External system services are provided by an external provider, and the organization has no direct control over the implementation of the required controls or the assessment of control effectiveness. Organizations establish relationships with external service providers in a variety of ways, including through business partnerships, contracts, interagency agreements, lines of business arrangements, licensing agreements, joint ventures, and supply chain exchanges. The responsibility for managing risks from the use of external system services remains with authorizing officials. For services external to organizations, a chain of trust requires that organizations establish and retain a certain level of confidence that each provider in the consumer-provider relationship provides adequate protection for the services rendered. The extent and nature of this chain of trust vary based on relationships between organizations and the external providers. Organizations document the basis for the trust relationships so that the relationships can be monitored. External system services documentation includes government, service providers, end user security roles and responsibilities, and service-level agreements.

Service-level agreements define the expectations of performance for implemented controls, describe measurable outcomes, and identify remedies and response requirements for identified instances of noncompliance.

Related Controls: AC-20, CA-3, CP-2, IR-4, IR-7, PL-10, PL-11, PS-7, SA-2, SA-4, SR-3, SR- 5.

Control Enhancements:

(2) EXTERNAL SYSTEM SERVICES | IDENTIFICATION OF FUNCTIONS, PORTS, PROTOCOLS, AND SERVICES

[Priority 2]

Control:

Require providers of the following external system services to identify the functions, ports, protocols, and other services required for the use of such services: any system with a local, network, or remote connection to an agency information system.

Discussion: Information from external service providers regarding the specific functions, ports, protocols, and services used in the provision of such services can be useful when the need arises to understand the trade-offs involved in restricting certain functions and services or blocking certain ports and protocols.

Related Controls: CM-6, CM-7.

SA-10 DEVELOPER CONFIGURATION MANAGEMENT

[Priority 2]

Control:

Require the developer of the system, system component, or system service to:

- a. Perform configuration management during system, component, or service during design, development, implementation, operation, and disposal;
- b. Document, manage, and control the integrity of changes to security configuration, network diagrams, and system components (hardware, software, firmware) by implementing access restrictions such as least privilege for changes;
- c. Implement only organization-approved changes to the system, component, or service;
- d. Document approved changes to the system, component, or service and the potential security and privacy impacts of such changes; and
- e. Track security flaws and flaw resolution within the system, component, or service and report findings to the individual(s) with information security responsibilities and an individual(s) with system and services acquisition responsibilities.

Discussion: Organizations consider the quality and completeness of configuration management activities conducted by developers as direct evidence of applying effective security controls.

Controls include protecting the master copies of material used to generate security-relevant portions of the system hardware, software, and firmware from unauthorized modification or destruction. Maintaining the integrity of changes to the system, system component, or system service requires strict configuration control throughout the system development life cycle to track authorized changes and prevent unauthorized changes.

The configuration items that are placed under configuration management include the formal model; the functional, high-level, and low-level design specifications; other design data; implementation documentation; source code and hardware schematics; the current running version of the object code; tools for comparing new versions of security-relevant hardware descriptions and source code with previous versions; and test fixtures and documentation.

Depending on the mission and business needs of organizations and the nature of the contractual relationships in place, developers may provide configuration management support during the operations and maintenance stage of the system development life cycle.

Related Controls: CM-2, CM-3, CM-4, CM-7, CM-9, SA-4, SA-5, SA-8, SA-15, SI-2, SR-3, SR-5, SR-6.

SA-11 DEVELOPER TESTING AND EVALUATION

[Priority 2]

Control:

Require the developer of the system, system component, or system service, at all post-design stages of the system development life cycle, to:

- a. Develop and implement a plan for ongoing security and privacy control assessments;

- b. Perform system and regression testing/evaluation at a level of comprehensive testing;
- c. Produce evidence of the execution of the assessment plan and the results of the testing and evaluation;
- d. Implement a verifiable flaw remediation process; and
- e. Correct flaws identified during testing and evaluation.

Discussion: Developmental testing and evaluation confirms that the required controls are implemented correctly, operating as intended, enforcing the desired security and privacy policies, and meeting established security and privacy requirements. Security properties of systems and the privacy of individuals may be affected by the interconnection of system components or changes to those components. The interconnections or changes—including upgrading or replacing applications, operating systems, and firmware—may adversely affect previously implemented controls. Ongoing assessment during development allows for additional types of testing and evaluation that developers can conduct to reduce or eliminate potential flaws.

Testing custom software applications may require approaches, such as manual code review, security architecture review, and penetration testing, as well as static analysis, dynamic analysis, binary analysis, or a hybrid of the three analysis approaches.

Developers can use the analysis approaches, along with security instrumentation and fuzzing, in a variety of tools and in source code reviews. The security and privacy assessment plans include the specific activities that developers plan to carry out, including the types of analyses, testing, evaluation, and reviews of software and firmware components; the degree of rigor to be applied; the frequency of the ongoing testing and evaluation; and the types of artifacts produced during those processes. The depth of testing and evaluation refers to the rigor and level of detail associated with the assessment process. The coverage of testing and evaluation refers to the scope (i.e., number and type) of the artifacts included in the assessment process. Contracts specify the acceptance criteria for security and privacy assessment plans, flaw remediation processes, and the evidence that the plans and processes have been diligently applied. Methods for reviewing and protecting assessment plans, evidence, and documentation are commensurate with the security category or classification level of the system. Contracts may specify protection requirements for documentation.

Related Controls: CA-2, CA-7, CM-4, SA-3, SA-4, SA-5, SA-8, SA-15, SI-2, SR-5, SR-6.

SA-15 DEVELOPMENT PROCESS, STANDARDS, AND TOOLS

[Priority 3]

Control:

- a. Require the developer of the system, system component, or system service to follow a documented development process that:
 - 1. Explicitly addresses security and privacy requirements;
 - 2. Identifies the standards and tools used in the development process;

3. Documents the specific tool options and tool configurations used in the development process; and
 4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and
- b. Review the development process, standards, tools, tool options, and tool configurations to determine if the process, standards, tools, tool options and tool configurations selected and employed can satisfy security and privacy requirements during design, development, implementation, operation, and disposal.

Discussion: Development tools include programming languages and computer-aided design systems. Reviews of development processes include the use of maturity models to determine the potential effectiveness of such processes. Maintaining the integrity of changes to tools and processes facilitates effective supply chain risk assessment and mitigation. Such integrity requires configuration control throughout the system development life cycle to track authorized changes and prevent unauthorized changes.

Related Controls: MA-6, SA-3, SA-4, SA-8, SA-10, SA-11, SR-3, SR-5, SR-6.

Control Enhancements:

(1) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS |CRITICALITY ANALYSIS

[Priority 3]

Control:

Require the developer of the system, system component, or system service to perform a criticality analysis:

- a. At the following decision points in the system development life cycle: design, development, implementation, and operational; and
- b. At the following level of rigor: comprehensive testing.

Discussion: Criticality analysis performed by the developer provides input to the criticality analysis performed by organizations. Developer input is essential to organizational criticality analysis because organizations may not have access to detailed design documentation for system components that are developed as commercial off-the-shelf products. Such design documentation includes functional specifications, high-level designs, low-level designs, source code, and hardware schematics. Criticality analysis is important for organizational systems that are designated as high value assets. High value assets can be moderate- or high-impact systems due to heightened adversarial interest or potential adverse effects on the federal enterprise.

Developer input is especially important when organizations conduct supply chain criticality analyses.

Related Controls: RA-9.

SA-22 UNSUPPORTED SYSTEM COMPONENTS

[Priority 2]

Control:

- a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or
- b. Provide the following options for alternative sources for continued support for unsupported components: original manufacturer support, or original contracted vendor support.

Discussion: Support for system components includes software patches, firmware updates, replacement parts, and maintenance contracts. An example of unsupported components includes when vendors no longer provide critical software patches or product updates, which can result in an opportunity for adversaries to exploit weaknesses in the installed components.

Exceptions to replacing unsupported system components include systems that provide critical mission or business capabilities where newer technologies are not available or where the systems are so isolated that installing replacement components is not an option.

Alternative sources for support address the need to provide continued support for system components that are no longer supported by the original manufacturers, developers, or vendors when such components remain essential to organizational mission and business functions. If necessary, organizations can establish in-house support by developing customized patches for critical software components or, alternatively, obtain the services of external providers who provide ongoing support for the designated unsupported components through contractual relationships. Such contractual relationships can include open-source software value-added vendors. The increased risk of using unsupported system components can be mitigated, for example, by prohibiting the connection of such components to public or uncontrolled networks or implementing other forms of isolation.

Related Controls: PL-2, SA-3.

SYSTEMS AND COMMUNICATIONS PROTECTION (SC)

Examples of systems and communications safeguards range from boundary and transmission protection to securing an agency's virtualized environment. In addition, applications, services, or information systems must have the capability to ensure system integrity through the detection and protection against unauthorized changes to software and information. This section details the requirements for protecting systems and communications infrastructures.

SC-1 POLICY AND PROCEDURES

[Priority 2]

Control:

- a. Develop, document, and disseminate to organizational personnel with system and communications protection responsibilities:
 1. Agency-level system and communications protection policy that:
 - (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 - (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
 2. Procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls;
- b. Designate organizational personnel with information security responsibilities to manage the development, documentation, and dissemination of the system and communications protection policy and procedures; and
- c. Review and update the current system and communications protection:
 1. Policy annually and following any changes and security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI; and
 2. Procedures annually and following any changes and security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.

Discussion: System and communications protection policy and procedures address the controls in the SC family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of system and communications protection policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may

precipitate an update to system and communications protection policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PS-8, SA-8, SI-12.

SC-2 SEPARATION OF SYSTEM AND USER FUNCTIONALITY

[Existing] [Priority 2]

Control:

Separate user functionality, including user interface services, from system management functionality.

Discussion: System management functionality includes functions that are necessary to administer databases, network components, workstations, or servers. These functions typically require privileged user access. The separation of user functions from system management functions is physical or logical. Organizations may separate system management functions from user functions by using different computers, instances of operating systems, central processing units, or network addresses; by employing virtualization techniques; or some combination of these or other methods. Separation of system management functions from user functions includes web administrative interfaces that employ separate authentication methods for users of any other system resources. Separation of system and user functions may include isolating administrative interfaces on different domains and with additional access controls. The separation of system and user functionality can be achieved by applying the systems security engineering design principles in SA-8.

Related Controls: AC-6, SA-4, SA-8, SC-7, SC-22, SC-39.

SC-4 INFORMATION IN SHARED SYSTEM RESOURCES

[Existing] [Priority 2]

Control:

Prevent unauthorized and unintended information transfer via shared system resources.

Discussion: Preventing unauthorized and unintended information transfer via shared system resources stops information produced by the actions of prior users or roles (or the actions of processes acting on behalf of prior users or roles) from being available to current users or roles (or current processes acting on behalf of current users or roles) that obtain access to shared system resources after those resources have been released back to the system. Information in shared system resources also applies to encrypted representations of information. In other contexts, control of information in shared system resources is referred to as object reuse and residual information protection. Information in shared system resources does not address information remanence, which refers to the residual representation of data that has been nominally deleted; covert channels (including storage and timing channels), where shared system resources are

manipulated to violate information flow restrictions; or components within systems for which there are only single users or roles.

Related Controls: AC-3, AC-4, SA-8.

SC-5 DENIAL-OF-SERVICE PROTECTION

[Priority 2]

Control:

- a. Protect against or limit the effects of the following types of denial-of-service events: distributed denial of service, DNS Denial of Service, etc.; and
- b. Employ the following controls to achieve the denial-of-service objective: boundary protection devices and intrusion detection or prevention devices.

Discussion: Denial-of-service events may occur due to a variety of internal and external causes, such as an attack by an adversary or a lack of planning to support organizational needs with respect to capacity and bandwidth. Such attacks can occur across a wide range of network protocols (e.g., IPv4, IPv6). A variety of technologies are available to limit or eliminate the origination and effects of denial-of-service events. For example, boundary protection devices can filter certain types of packets to protect system components on internal networks from being directly affected by or the source of denial-of-service attacks. Employing increased network capacity and bandwidth combined with service redundancy also reduces the susceptibility to denial-of-service events.

Related Controls: CP-2, IR-4, SC-7.

SC-7 BOUNDARY PROTECTION

[Existing] [Priority 1]

Control:

- a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system;
- b. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal organizational networks; and
- c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.

Discussion: Managed interfaces include gateways, routers, firewalls, guards, network-based malicious code analysis, virtualization systems, or encrypted tunnels implemented within a security architecture. Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones or DMZs. Restricting or prohibiting interfaces within organizational systems includes restricting external web traffic to designated web servers within managed interfaces, prohibiting external traffic that appears to be spoofing internal addresses, and prohibiting internal traffic that appears to be spoofing external addresses. [SP 800-

189] provides additional information on source address validation techniques to prevent ingress and egress of traffic with spoofed addresses. Commercial telecommunications services are provided by network components and consolidated management systems shared by customers. These services may also include third party-provided access lines and other service elements. Such services may represent sources of increased risk despite contract security provisions. Boundary protection may be implemented as a common control for all or part of an organizational network such that the boundary to be protected is greater than a system-specific boundary (i.e., an authorization boundary).

Related Controls: AC-4, AC-17, AC-18, AC-19, AC-20, CA-3, CM-2, CM-4, CM-7, CM-10, CP-8, CP-10, IR-4, MA-4, PE-3, PL-8, SA-8, SC-5.

Control Enhancements:

(3) BOUNDARY PROTECTION | ACCESS POINTS

[Priority 1]

Control:

Limit the number of external network connections to the system.

Discussion: Limiting the number of external network connections facilitates monitoring of inbound and outbound communications traffic. A Trusted Internet Connection (TIC) initiative is an example of a federal guideline that requires limits on the number of external network connections. Limiting the number of external network connections to the system is important during transition periods from older to newer technologies (e.g., transitioning from IPv4 to IPv6 network protocols). Such transitions may require implementing the older and newer technologies simultaneously during the transition period and thus increase the number of access points to the system.

Related Controls: None.

(4) BOUNDARY PROTECTION | EXTERNAL TELECOMMUNICATIONS SERVICES

[Priority 1]

Control:

- a. Implement a managed interface for each external telecommunication service;
- b. Establish a traffic flow policy for each managed interface;
- c. Protect the confidentiality and integrity of the information being transmitted across each interface;
- d. Document each exception to the traffic flow policy with a supporting mission or business need and duration of that need;
- e. Review exceptions to the traffic flow policy annually, after any incident, and after any major changes impacting the information system, while removing exceptions that are no longer supported by an explicit mission or business need;
- f. Prevent unauthorized exchange of control plane traffic with external networks;

- g. Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks; and
- h. Filter unauthorized control plane traffic from external networks.

Discussion: External telecommunications services can provide data and/or voice communications services. Examples of control plane traffic include Border Gateway Protocol (BGP) routing, Domain Name System (DNS), and management protocols. See [SP 800-189] for additional information on the use of the resource public key infrastructure (RPKI) to protect BGP routes and detect unauthorized BGP announcements.

Related Controls: AC-3, SC-8, SC-20, SC-21, SC-22.

(5) BOUNDARY PROTECTION | DENY BY DEFAULT — ALLOW BY EXCEPTION

[Priority 1]

Control:

Deny network communications traffic by default and allow network communications traffic by exception at boundary devices for information systems used to process, store, or transmit CJL.

Discussion: Denying by default and allowing by exception applies to inbound and outbound network communications traffic. A deny-all, permit-by-exception network communications traffic policy ensures that only those system connections that are essential and approved are allowed. Deny by default, allow by exception also applies to a system that is connected to an external system.

Related Controls: None.

(7) BOUNDARY PROTECTION | SPLIT TUNNELING FOR REMOTE DEVICES

[Priority 1]

Control:

Prevent split tunneling for remote devices connecting to organizational systems.

Discussion: Split tunneling is the process of allowing a remote user or device to establish a non-remote connection with a system and simultaneously communicate via some other connection to a resource in an external network. This method of network access enables a user to access remote devices and simultaneously, access uncontrolled networks. Split tunneling might be desirable by remote users to communicate with local system resources, such as printers or file servers. However, split tunneling can facilitate unauthorized external connections, making the system vulnerable to attack and to exfiltration of organizational information. Split tunneling can be prevented by disabling configuration settings that allow such capability in remote devices and by preventing those configuration settings from being configurable by users. Prevention can also be achieved by the detection of split tunneling (or of configuration settings that allow split tunneling) in the remote device, and by prohibiting the connection if the remote device is using split tunneling. A virtual private network (VPN) can be used to securely provision a split tunnel. A securely provisioned VPN includes locking connectivity to exclusive, managed, and named environments, or to a specific set of pre-approved addresses, without user control.

Related Controls: None.

(8) BOUNDARY PROTECTION | ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS

[Existing] [Priority 1]

Control:

Route all internal communications traffic that may be proxied, except traffic specifically exempted by organizational personnel with information security responsibilities, to all untrusted networks through authenticated proxy servers at managed interfaces.

Discussion: External networks are networks outside of organizational control. A proxy server is a server (i.e., system or application) that acts as an intermediary for clients requesting system resources from non-organizational or other organizational servers. System resources that may be requested include files, connections, web pages, or services. Client requests established through a connection to a proxy server are assessed to manage complexity and provide additional protection by limiting direct connectivity. Web content filtering devices are one of the most common proxy servers that provide access to the Internet. Proxy servers can support the logging of Transmission Control Protocol sessions and the blocking of specific Uniform Resource Locators, Internet Protocol addresses, and domain names. Web proxies can be configured with organization-defined lists of authorized and unauthorized websites. Note that proxy servers may inhibit the use of virtual private networks (VPNs) and create the potential for “man-in-the-middle” attacks (depending on the implementation).

Related Controls: AC-3.

(24) BOUNDARY PROTECTION | PERSONALLY IDENTIFIABLE INFORMATION

[Priority 1]

Control:

For systems that process personally identifiable information:

- a. Apply the following processing rules to data elements of personally identifiable information: all applicable laws, executive orders, directives, regulations, policies, standards, and guidelines;
- b. Monitor for permitted processing at the external interfaces to the system and at key internal boundaries within the system;
- c. Document each processing exception; and
- d. Review and remove exceptions that are no longer supported.

Discussion: Managing the processing of personally identifiable information is an important aspect of protecting an individual’s privacy. Applying, monitoring for, and documenting exceptions to processing rules ensure that personally identifiable information is processed only in accordance with established privacy requirements.

Related Controls: None.

SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY

[Existing] [Priority 2]

Control:

Protect the confidentiality and integrity of transmitted information.

Metadata derived from unencrypted CJI shall be protected in the same manner as CJI and shall not be used for any advertising or other commercial purposes by any cloud service provider or other associated entity.

Discussion: Protecting the confidentiality and integrity of transmitted information applies to internal and external networks as well as any system components that can transmit information, including servers, notebook computers, desktop computers, mobile devices, printers, copiers, scanners, facsimile machines, and radios. Unprotected communication paths are exposed to the possibility of interception and modification. Protecting the confidentiality and integrity of information can be accomplished by physical or logical means. Physical protection can be achieved by using protected distribution systems. A protected distribution system is a wireline or fiber-optics telecommunications system that includes terminals and adequate electromagnetic, acoustical, electrical, and physical controls to permit its use for the unencrypted transmission of classified information. Logical protection can be achieved by employing encryption techniques. Organizations that rely on commercial providers who offer transmission services as commodity services rather than as fully dedicated services may find it difficult to obtain the necessary assurances regarding the implementation of needed controls for transmission confidentiality and integrity. In such situations, organizations determine what types of confidentiality or integrity services are available in standard, commercial telecommunications service packages. If it is not feasible to obtain the necessary controls and assurances of control effectiveness through appropriate contracting vehicles, organizations can implement appropriate compensating controls. The agency may permit limited use of metadata derived from unencrypted CJI when specifically approved by the agency and its “intended use” is detailed within the service agreement. Such authorized uses of metadata may include but are not limited to the following: spam and spyware filtering, data loss prevention, spillage reporting, transaction logs (events and content—similar to the AU controls), data usage/indexing metrics, and diagnostic/syslog data.

Related Controls: AC-17, AC-18, IA-3, IA-8, MA-4, PE-4, SA-4, SA-8, SC-7, SC-20, SC-23, SC-28.

Control Enhancements:

(1) TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC PROTECTION

[Existing] [Priority 2]

Control:

Implement cryptographic mechanisms to prevent unauthorized disclosure and detect unauthorized changes or access to CJI during transmission.

Discussion: Encryption protects information from unauthorized disclosure and modification during transmission. Cryptographic mechanisms that protect the confidentiality and integrity of information during transmission include TLS and IPSec. Cryptographic mechanisms used to

protect information integrity include cryptographic hash functions that have applications in digital signatures, checksums, and message authentication codes.

Related Controls: SC-12, SC-13.

SC-10 NETWORK DISCONNECT

[Priority 3]

Control:

Terminate the network connection associated with a communications session at the end of the session or after one (1) hour of inactivity.

NOTE: In the interest of safety, devices that are: (1) part of a criminal justice conveyance; or (2) used to perform dispatch functions and located within a physically secure location; or (3) terminals designated solely for the purpose of receiving alert notifications (i.e., receive only terminals or ROT) and used within physically secure location facilities that remain staffed when in operation, are exempt from this requirement.

Discussion: Network disconnect applies to internal and external networks. Terminating network connections associated with specific communications sessions includes de-allocating TCP/IP address or port pairs at the operating system level and de-allocating the networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. Periods of inactivity may be established by organizations and include time periods by type of network access or for specific network accesses.

Related Controls: AC-17, SC-23.

SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

[Existing] [Priority 2]

Control:

Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: encryption key generation, distribution, storage, access, and destruction is controlled by the agency.

Discussion: Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. Organizations define key management requirements in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and specify appropriate options, parameters, and levels. Organizations manage trust stores to ensure that only approved trust anchors are part of such trust stores. This includes certificates with visibility external to organizational systems and certificates related to the internal operations of systems. [NIST CMVP] and [NIST CAVP] provide additional information on validated cryptographic modules and algorithms that can be used in cryptographic key management and establishment.

Related Controls: AC-17, AU-9, CM-3, IA-3, IA-7, SA-4, SA-8, SA-9, SC-8, SC-12, SC-13, SC-17, SC-20, SI-3, SI-7.

SC-13 CRYPTOGRAPHIC PROTECTION

[Existing] [Priority 2]

Control:

- a. Determine the use of encryption for CJI in-transit when outside a physically secure location; and
- b. Implement the following types of cryptography required for each specified cryptographic use: cryptographic modules which are Federal Information Processing Standard (FIPS) 140-3 certified, or FIPS validated algorithm for symmetric key encryption and decryption (FIPS 197 [AES]), with a symmetric cipher key of at least 128-bit strength for CJI in-transit.

NOTE: Subsequent versions of approved cryptographic modules that are under current review for FIPS 140-3 compliancy can be used in the interim until certification is complete. FIPS 140-2 certificates will not be acceptable after September 21, 2026.

Discussion: Cryptography can be employed to support a variety of security solutions, including the protection of classified information and controlled unclassified information, the provision and implementation of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances but lack the necessary formal access approvals. Cryptography can also be used to support random number and hash generation. Generally applicable cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography. For example, organizations that need to protect classified information may specify the use of NSA-approved cryptography. Organizations that need to provision and implement digital signatures may specify the use of FIPS-validated cryptography. Cryptography is implemented in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Related Controls: AC-2, AC-3, AC-7, AC-17, AC-18, AC-19, AU-9, CM-11, CP-9, IA-3, IA-5, IA-7, MA-4, MP-2, MP-4, MP-5, SA-4, SA-8, SA-9, SC-8, SC-12, SC-20, SC-23, SC-28, SI-3, SI-7.

SC-15 COLLABORATIVE COMPUTING DEVICES AND APPLICATIONS

[Priority 2]

Control:

- a. Prohibit remote activation of collaborative computing devices and applications; and
- b. Provide an explicit indication of use to users physically present at the devices.

Discussion: Collaborative computing devices and applications include remote meeting devices and applications, networked white boards, cameras, and microphones. The explicit indication of use includes signals to users when collaborative computing devices and applications are activated.

Related Controls: AC-21.

SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES

[Existing] [Priority 2]

Control:

- a. Issue public key certificates under an agency-level certificate authority or obtain public key certificates from an approved service provider; and
- b. Include only approved trust anchors in trust stores or certificate stores managed by the organization.

Discussion: Public key infrastructure (PKI) certificates are certificates with visibility external to organizational systems and certificates related to the internal operations of systems, such as application-specific time services. In cryptographic systems with a hierarchical structure, a trust anchor is an authoritative source (i.e., a certificate authority) for which trust is assumed and not derived. A root certificate for a PKI system is an example of a trust anchor. A trust store or certificate store maintains a list of trusted root certificates.

Related Controls: IA-5, SC-12.

SC-18 MOBILE CODE

[Priority 3]

Control:

- a. Define acceptable and unacceptable mobile code and mobile code technologies; and
- b. Authorize, monitor, and control the use of mobile code within the system.

Discussion: Mobile code includes any program, application, or content that can be transmitted across a network (e.g., embedded in an email, document, or website) and executed on a remote system. Decisions regarding the use of mobile code within organizational systems are based on the potential for the code to cause damage to the systems if used maliciously. Mobile code technologies include Java applets, JavaScript, HTML5, WebGL, and VBScript. Usage restrictions and implementation guidelines apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations and devices, including notebook computers and smart phones. Mobile code policy and procedures address specific actions taken to prevent the development, acquisition, and introduction of unacceptable mobile code within organizational systems, including requiring mobile code to be digitally signed by a trusted source.

Related Controls: AU-2, AU-12, CM-2, CM-6, SI-3.

SC-20 SECURE NAME/ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)

[Priority 2]

Control:

- a. Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and
- b. Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

Discussion: Providing authoritative source information enables external clients, including remote Internet clients, to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service. Systems that provide name and address resolution services include domain name system (DNS) servers. Additional artifacts include DNS Security Extensions (DNSSEC) digital signatures and cryptographic keys. Authoritative data includes DNS resource records. The means for indicating the security status of child zones include the use of delegation signer resource records in the DNS. Systems that use technologies other than the DNS to map between host and service names and network addresses provide other means to assure the authenticity and integrity of response data.

Related Controls: SC-8, SC-12, SC-13, SC-21, SC-22.

SC-21 SECURE NAME/ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)

[Priority 2]

Control:

Request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

Discussion: Each client of name resolution services either performs this validation on its own or has authenticated channels to trusted validation providers. Systems that provide name and address resolution services for local clients include recursive resolving or caching domain name system (DNS) servers. DNS client resolvers either perform validation of DNSSEC signatures, or clients use authenticated channels to recursive resolvers that perform such validations. Systems that use technologies other than the DNS to map between host and service names and network addresses provide some other means to enable clients to verify the authenticity and integrity of response data.

Related Controls: SC-20, SC-22.

SC-22 ARCHITECTURE AND PROVISIONING FOR NAME/ADDRESS RESOLUTION SERVICE

[Priority 2]

Control:

Ensure the systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal and external role separation.

Discussion: Systems that provide name and address resolution services include domain name system (DNS) servers. To eliminate single points of failure in systems and enhance redundancy, organizations employ at least two authoritative domain name system servers—one configured as the primary server and the other configured as the secondary server. Additionally, organizations typically deploy the servers in two geographically separated network subnetworks (i.e., not located in the same physical facility). For role separation, DNS servers with internal roles only process name and address resolution requests from within organizations (i.e., from internal clients). DNS servers with external roles only process name and address resolution information requests from clients external to organizations (i.e., on external networks, including the Internet). Organizations specify clients that can access authoritative DNS servers in certain roles (e.g., by address ranges and explicit lists).

Related Controls: SC-2, SC-20, SC-21.

SC-23 SESSION AUTHENTICITY

[Priority 2]

Control:

Protect the authenticity of communications sessions.

Discussion: Protecting session authenticity addresses communications protection at the session level, not at the packet level. Such protection establishes grounds for confidence at both ends of communications sessions in the ongoing identities of other parties and the validity of transmitted information. Authenticity protection includes protecting against “man-in-the-middle” attacks, session hijacking, and the insertion of false information into sessions.

Related Controls: SC-8, SC-10.

SC-28 PROTECTION OF INFORMATION AT REST

[Existing] [Priority 2]

Control:

Protect the confidentiality and integrity of the following information at rest: CJI when outside physically secure locations using cryptographic modules which are certified FIPS 140-3 with a symmetric cipher key of at least 128-bit strength, or FIPS 197 with a symmetric cipher key of at least 256-bit strength.

Metadata derived from unencrypted CJI shall be protected in the same manner as CJI and shall not be used for any advertising or other commercial purposes by any cloud service provider or other associated entity.

The storage of CJI, regardless of encryption status, shall only be permitted in cloud environments (e.g., government or third-party/commercial datacenters, etc.) which reside within the physical boundaries of APB-member country (i.e., United States, U.S. territories, Indian Tribes, and Canada) and are under legal authority of an APB-member agency (i.e., United States–federal/state/territory, Indian Tribe, or the Royal Canadian Mounted Police).

Note: This restriction does not apply to exchanges of CJI with foreign government agencies under international exchange agreements (e.g., the Preventing and Combating Serious Crime agreements, fugitive extracts, and exchanges made for humanitarian and criminal investigatory purposes in particular circumstances).

Discussion: Information at rest refers to the state of information when it is not in process or in transit and is located on system components. Such components include internal or external hard disk drives, storage area network devices, or databases. However, the focus of protecting information at rest is not on the type of storage device or frequency of access but rather on the state of the information. Information at rest addresses the confidentiality and integrity of information and covers user information and system information. System-related information that requires protection includes configurations or rule sets for firewalls, intrusion detection and prevention systems, filtering routers, and authentication information. Organizations may employ different mechanisms to achieve confidentiality and integrity protections, including the use of cryptographic mechanisms and file share scanning. Integrity protection can be achieved, for example, by implementing write-once-read-many (WORM) technologies. When adequate protection of information at rest cannot otherwise be achieved, organizations may employ other controls, including frequent scanning to identify malicious code at rest and secure offline storage in lieu of online storage. The agency may permit limited use of metadata derived from unencrypted CJI when specifically approved by the agency and its “intended use” is detailed within the service agreement. Such authorized uses of metadata may include but are not limited to the following: spam and spyware filtering, data loss prevention, spillage reporting, transaction logs (events and content–similar to the AU controls), data usage/indexing metrics, and diagnostic/syslog data.

Related Controls: AC-3, AC-4, AC-6, AC-19, CA-7, CM-3, CM-5, CM-6, CP-9, MP-4, MP-5, PE-3, SC-8, SC-12, SC-13, SI-3, SI-7, SI-16.

Control Enhancements:

(1) PROTECTION OF INFORMATION AT REST | CRYPTOGRAPHIC PROTECTION

[Existing] [Priority 2]

Control:

Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on information systems and digital media outside physically secure locations: CJI.

Discussion: The selection of cryptographic mechanisms is based on the need to protect the confidentiality and integrity of organizational information. The strength of mechanism is commensurate with the security category or classification of the information. Organizations have the flexibility to encrypt information on system components or media or encrypt data structures, including files, records, or fields.

Related Controls: AC-19, SC-12, SC-13.

SC-39 PROCESS ISOLATION

[Existing] [Priority 2]

Control:

Maintain a separate execution domain for each executing system process.

Discussion: Systems can maintain separate execution domains for each executing process by assigning each process a separate address space. Each system process has a distinct address space so that communication between processes is performed in a manner controlled through the security functions, and one process cannot modify the executing code of another process. Maintaining separate execution domains for executing processes can be achieved, for example, by implementing separate address spaces. Process isolation technologies, including sandboxing or virtualization, logically separate software and firmware from other software, firmware, and data. Process isolation helps limit the access of potentially untrusted software to other system resources. The capability to maintain separate execution domains is available in commercial operating systems that employ multi-state processor technologies.

Related Controls: AC-3, AC-4, AC-6, SA-8, SC-2, SI-16.

Figure 14 – System and Communications Protection and Information Integrity Use Cases

Use Case 1 – A Local Police Department’s Information Systems & Communications Protections

A local police department implemented a replacement CAD system within a physically secure location that was authorized to process CJI using a FIPS 140-2 encrypted VPN tunnel over the Internet to the state’s CSA. In addition to the policies, physical and personnel controls already in place, the police department employed firewalls both at their border and at key points within their network, intrusion detection systems, a patch-management strategy that included automatic patch updates where possible, virus scanners, spam and spyware detection mechanisms that update signatures automatically, and subscribed to various security alert mailing lists and addressed vulnerabilities raised through the alerts as needed.

Use Case 2 – Faxing from a Single/Multi-function Device over a Traditional Telephone Line

A dispatcher from county A runs a NCIC query on an individual. The results are printed and then sent to an adjoining county using a single/multi-function device with facsimile capability. For faxing, the device is only connected to a traditional telephone line as is the device at the receiving county. Encryption of a document containing CJI is not required because the document travels over a traditional telephone line.

Use Case 3 – Faxing from a Multi-function Device over a Network

A dispatcher from city A runs a NCIC query on an individual. The results are printed and the dispatcher uses a multi-function copier to fax the file to a city in another state. The dispatcher enters the fax number of the receiver and sends the document. The document containing CJI is automatically converted to a digital file and routed to the receiver over the agency network and the Internet. Because the device uses a network and the Internet for transmitting documents containing CJI, encryption in transit using FIPS 140-2 certified 128 bit symmetric encryption is required.

SYSTEM AND INFORMATION INTEGRITY (SI)

SI-1 POLICY AND PROCEDURES

[Priority 2]

Control:

- a. Develop, document, and disseminate to all organizational personnel with system and information integrity responsibilities and information system owners:
 1. Agency-level system and information integrity policy that:
 - (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 - (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
 2. Procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls;
- b. Designate organizational personnel with system and information integrity responsibilities to manage the development, documentation, and dissemination of the system and information integrity policy and procedures; and
- c. Review and update the current system and information integrity:
 1. Policy annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI; and
 2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.

Discussion: System and information integrity policy and procedures address the controls in the SI family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of system and information integrity policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to system and information integrity policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PS-8, SA-8, SI-12.

SI-2 FLAW REMEDIATION

[Existing] [Priority 1]

Control:

- a. Identify, report, and correct system flaws;
- b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
- c. Install security-relevant software and firmware updates within the number of days listed after the release of the updates;
 - Critical – 15 days
 - High – 30 days
 - Medium – 60 days
 - Low – 90 days; and
- d. Incorporate flaw remediation into the organizational configuration management process.

Discussion: The need to remediate system flaws applies to all types of software and firmware. Organizations identify systems affected by software flaws, including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security and privacy responsibilities. Security-relevant updates include patches, service packs, and malicious code signatures. Organizations also address flaws discovered during assessments, continuous monitoring, incident response activities, and system error handling. By incorporating flaw remediation into configuration management processes, required remediation actions can be tracked and verified.

Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of risk factors, including the security category of the system, the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw), the organizational risk tolerance, the mission supported by the system, or the threat environment. Some types of flaw remediation may require more testing than other types. Organizations determine the type of testing needed for the specific type of flaw remediation activity under consideration and the types of changes that are to be configuration-managed. In some situations, organizations may determine that the testing of software or firmware updates is not necessary or practical, such as when implementing simple malicious code signature updates. In testing decisions, organizations consider whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures.

Related Controls: CA-5, CM-3, CM-4, CM-5, CM-6, CM-8, MA-2, RA-5, SA-8, SA-10, SA-11, SI-3, SI- 5, SI-7, SI-11.

Control Enhancements:

(2) FLAW REMEDIATION | AUTOMATED FLAW REMEDIATION STATUS

[Priority 1]

Control:

Determine if system components have applicable security-relevant software and firmware updates installed using vulnerability scanning tools at least quarterly or following any security incidents involving CJI or systems used to process, store, or transmit CJI.

Discussion: Automated mechanisms can track and determine the status of known flaws for system components.

Related Controls: CA-7, SI-4.

SI-3 MALICIOUS CODE PROTECTION

[Existing] [Priority 1]

Control:

- a. Implement signature-based malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;
- b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;
- c. Configure malicious code protection mechanisms to:
 1. Perform periodic scans of the system at least daily and real-time scans of files from external sources at network entry and exit points and on all servers and endpoint devices as the files are downloaded, opened, or executed in accordance with organizational policy; and
 2. Block or quarantine malicious code, take mitigating action(s), and when necessary, implement incident response procedures; and send alert to system/network administrators and/or organizational personnel with information security responsibilities in response to malicious code detection; and
- d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.

Discussion: System entry and exit points include firewalls, remote access servers, workstations, electronic mail servers, web servers, proxy servers, notebook computers, and mobile devices. Malicious code includes viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats contained within compressed or hidden files or hidden in files using techniques such as steganography. Malicious code can be inserted into systems in a variety of ways, including by electronic mail, the World Wide Web, and portable storage devices. Malicious code insertions occur through the exploitation of system vulnerabilities. A variety of technologies and methods exist to limit or eliminate the effects of malicious code.

Malicious code protection mechanisms include both signature- and nonsignature-based technologies. Nonsignature-based detection mechanisms include artificial intelligence techniques that use heuristics to detect, analyze, and describe the characteristics or behavior of malicious

code and to provide controls against such code for which signatures do not yet exist or for which existing signatures may not be effective. Malicious code for which active signatures do not yet exist or may be ineffective includes polymorphic malicious code (i.e., code that changes signatures when it replicates). Nonsignature-based mechanisms also include reputation-based technologies. In addition to the above technologies, pervasive configuration management, comprehensive software integrity controls, and anti-exploitation software may be effective in preventing the execution of unauthorized code. Malicious code may be present in commercial off-the-shelf software as well as custom-built software and could include logic bombs, backdoors, and other types of attacks that could affect organizational mission and business functions.

In situations where malicious code cannot be detected by detection methods or technologies, organizations rely on other types of controls, including secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to ensure that software does not perform functions other than the functions intended. Organizations may determine that, in response to the detection of malicious code, different actions may be warranted. For example, organizations can define actions in response to malicious code detection during periodic scans, the detection of malicious downloads, or the detection of maliciousness when attempting to open or execute files.

Related Controls: AC-4, AC-19, CM-3, CM-8, IR-4, MA-3, MA-4, RA-5, SC-7, SC-23, SC- 28, SI-2, SI-4, SI-7, SI-8.

SI-4 SYSTEM MONITORING

[Priority 1]

Control:

- a. Monitor the system to detect:
 1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives:
 - a. Intrusion detection and prevention
 - b. Malicious code protection
 - c. Vulnerability scanning
 - d. Audit record monitoring
 - e. Network monitoring
 - f. Firewall monitoring;and
 2. Unauthorized local, network, and remote connections;
- b. Identify unauthorized use of the system through the following techniques and methods: event logging (ref. 5.4 Audit and Accountability);
- c. Invoke internal monitoring capabilities or deploy monitoring devices:

1. Strategically within the system to collect organization-determined essential information; and
 2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;
- d. Analyze detected events and anomalies;
 - e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;
 - f. Obtain legal opinion regarding system monitoring activities; and
 - g. Provide intrusion detection and prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring, and firewall monitoring software logs to organizational personnel with information security responsibilities weekly.

Discussion: System monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at external interfaces to the system. Internal monitoring includes the observation of events occurring within the system. Organizations monitor systems by observing audit activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives guide and inform the determination of the events. System monitoring capabilities are achieved through a variety of tools and techniques, including intrusion detection and prevention systems, malicious code protection software, scanning tools, audit record monitoring software, and network monitoring software.

Depending on the security architecture, the distribution and configuration of monitoring devices may impact throughput at key internal and external boundaries as well as at other locations across a network due to the introduction of network throughput latency. If throughput management is needed, such devices are strategically located and deployed as part of an established organization-wide security architecture. Strategic locations for monitoring devices include selected perimeter locations and near key servers and server farms that support critical applications. Monitoring devices are typically employed at the managed interfaces associated with controls SC-7 and AC-17. The information collected is a function of the organizational monitoring objectives and the capability of systems to support such objectives. Specific types of transactions of interest include Hypertext Transfer Protocol (HTTP) traffic that bypasses HTTP proxies. System monitoring is an integral part of organizational continuous monitoring and incident response programs, and output from system monitoring serves as input to those programs. System monitoring requirements, including the need for specific types of system monitoring, may be referenced in other controls (e.g., AC-2g, AC-17(1), CM-3f, CM-6d, MA-3a, MA-4a, SC-5(3)(b), SC-7a, SC-18b). Adjustments to levels of system monitoring are based on law enforcement information, intelligence information, or other sources of information. The legality of system monitoring activities is based on applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Related Controls: AC-2, AC-3, AC-4, AC-8, AC-17, AU-2, AU-6, AU-7, AU-9, AU-12, CA-7, CM-3, CM-6, CM-8, CM-11, IR-4, MA-3, MA-4, RA-5, SC-5, SC-7, SC-18, SI-3, SI-7, SR-10.

Control Enhancements:

(2) SYSTEM MONITORING | AUTOMATED TOOLS AND MECHANISMS FOR REAL-TIME ANALYSIS

[Existing] [Priority 1]

Control:

Employ automated tools and mechanisms to support near real-time analysis of events.

Discussion: Automated tools and mechanisms include host-based, network-based, transport-based, or storage-based event monitoring tools and mechanisms or security information and event management (SIEM) technologies that provide real-time analysis of alerts and notifications generated by organizational systems. Automated monitoring techniques can create unintended privacy risks because automated controls may connect to external or otherwise unrelated systems. The matching of records between these systems may create linkages with unintended consequences. Organizations assess and document these risks in their privacy impact assessment and make determinations that are in alignment with their privacy program plan.

Related Controls: None.

(4) SYSTEM MONITORING | INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC

[Existing] [Priority 1]

Control:

- a. Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic;
- b. Monitor inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions such as: the presence of malicious code or unauthorized use of legitimate code or credentials within organizational systems or propagating among system components, signaling to external systems, and the unauthorized exporting of information.

Discussion: Unusual or unauthorized activities or conditions related to system inbound and outbound communications traffic includes internal traffic that indicates the presence of malicious code or unauthorized use of legitimate code or credentials within organizational systems or propagating among system components, signaling to external systems, and the unauthorized exporting of information. Evidence of malicious code or unauthorized use of legitimate code or credentials is used to identify potentially compromised systems or system components.

Related Controls: None.

(5) SYSTEM MONITORING | SYSTEM-GENERATED ALERTS

[Existing] [Priority 1]

Control:

Alert organizational personnel with system monitoring responsibilities when the following system-generated indications of compromise or potential compromise occur: inappropriate or unusual activities with security or privacy implications.

Discussion: Alerts may be generated from a variety of sources, including audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers. Alerts can be automated and may be transmitted telephonically, by electronic mail messages, or by text messaging. Organizational personnel on the alert notification list can include system administrators, mission or business owners, system owners, information owners/stewards, senior agency information security officers, senior agency officials for privacy, system security officers, or privacy officers. In contrast to alerts generated by the system, alerts generated by organizations in SI-4(12) focus on information sources external to the system, such as suspicious activity reports and reports on potential insider threats.

Related Controls: AU-4, AU-5, PE-6.

SI-5 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

[Existing] [Priority 2]

Control:

- a. Receive system security alerts, advisories, and directives from external source(s) (e.g., CISA, Multi-State Information Sharing & Analysis Center [MS-ISAC], U.S. Computer Emergency Readiness Team [USCERT], hardware/software providers, federal/state advisories, etc.) on an ongoing basis;
- b. Generate internal security alerts, advisories, and directives as deemed necessary;
- c. Disseminate security alerts, advisories, and directives to: organizational personnel implementing, operating, maintaining, and using the system; and
- d. Implement security directives in accordance with established time frames, or notify the issuing organization of the degree of noncompliance.

Discussion: The Cybersecurity and Infrastructure Security Agency (CISA) generates security alerts and advisories to maintain situational awareness throughout the federal government. Security directives are issued by OMB or other designated organizations with the responsibility and authority to issue such directives. Compliance with security directives is essential due to the critical nature of many of these directives and the potential (immediate) adverse effects on organizational operations and assets, individuals, other organizations, and the Nation should the directives not be implemented in a timely manner. External organizations include supply chain partners, external mission or business partners, external service providers, and other peer or supporting organizations.

Related Controls: RA-5, SI-2.

SI-7 SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY

[Priority 1]

Control:

- a. Employ integrity verification tools to detect unauthorized changes to software, firmware, and

information systems that contain or process CJI; and

- b. Take the following actions when unauthorized changes to the software, firmware, and information are detected: notify organizational personnel responsible for software, firmware, and/or information integrity and implement incident response procedures as appropriate.

Discussion: Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity. Software includes operating systems (with key internal components, such as kernels or drivers), middleware, and applications. Firmware interfaces include Unified Extensible Firmware Interface (UEFI) and Basic Input/Output System (BIOS). Information includes personally identifiable information and metadata that contains security and privacy attributes associated with information. Integrity-checking mechanisms—including parity checks, cyclical redundancy checks, cryptographic hashes, and associated tools—can automatically monitor the integrity of systems and hosted applications.

Related Controls: AC-4, CM-3, CM-7, CM-8, MA-3, MA-4, RA-5, SA-8, SA-9, SA-10, SC-8, SC-12, SC-13, SC-28, SI-3, SR-3, SR-5, SR-6, SR-10, SR-11.

Control Enhancements:

(1) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY CHECKS

[Priority 1]

Control:

Perform an integrity check of software, firmware, and information systems that contain or process CJI at agency-defined transitional states or security relevant events at least weekly or in an automated fashion.

Discussion: Security-relevant events include the identification of new threats to which organizational systems are susceptible and the installation of new hardware, software, or firmware. Transitional states include system startup, restart, shutdown, and abort.

Related Controls: None.

(7) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRATION OF DETECTION AND RESPONSE

[Priority 1]

Control:

Incorporate the detection of the following unauthorized changes into the organizational incident response capability: unauthorized changes to established configuration setting or the unauthorized elevation of system privileges.

Discussion: Integrating detection and response helps to ensure that detected events are tracked, monitored, corrected, and available for historical purposes. Maintaining historical records is important for being able to identify and discern adversary actions over an extended time period and for possible legal actions. Security-relevant changes include unauthorized changes to established configuration settings or the unauthorized elevation of system privileges.

Related Controls: AU-2, AU-6, IR-4, IR-5, SI-4.

SI-8 SPAM PROTECTION

[Existing] [Priority 3]

Control:

- a. Employ spam protection mechanisms at system entry and exit points to detect and act on unsolicited messages; and
- b. Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

Discussion: System entry and exit points include firewalls, remote-access servers, electronic mail servers, web servers, proxy servers, workstations, notebook computers, and mobile devices. Spam can be transported by different means, including email, email attachments, and web accesses. Spam protection mechanisms include signature definitions.

Related Controls: SC-5, SC-7, SI-3, SI-4.

Control Enhancements:

(2) SPAM PROTECTION | AUTOMATIC UPDATES

[Priority 3]

Control:

Automatically update spam protection mechanisms at least daily.

Discussion: Using automated mechanisms to update spam protection mechanisms helps to ensure that updates occur on a regular basis and provide the latest content and protection capabilities.

Related Controls: None.

SI-10 INFORMATION INPUT VALIDATION

[Priority 1]

Control:

Check the validity of the following information inputs: all inputs to web/application servers, database servers, and any system or application input that might receive or process CJI.

Discussion: Checking the valid syntax and semantics of system inputs—including character set, length, numerical range, and acceptable values—verifies that inputs match specified definitions for format and content. For example, if the organization specifies that numerical values between 1-100 are the only acceptable inputs for a field in a given application, inputs of “387,” “abc,” or “%K%” are invalid inputs and are not accepted as input to the system. Valid inputs are likely to vary from field to field within a software application. Applications typically follow well-defined protocols that use structured messages (i.e., commands or queries) to communicate between software modules or system components. Structured messages can contain raw or unstructured data interspersed with metadata or control information. If software applications use attacker-

supplied inputs to construct structured messages without properly encoding such messages, then the attacker could insert malicious commands or special characters that can cause the data to be interpreted as control information or metadata. Consequently, the module or component that receives the corrupted output will perform the wrong operations or otherwise interpret the data incorrectly. Prescreening inputs prior to passing them to interpreters prevents the content from being unintentionally interpreted as commands. Input validation ensures accurate and correct inputs and prevents attacks such as cross-site scripting and a variety of injection attacks.

Related Controls: None.

SI-11 ERROR HANDLING

[Priority 3]

Control:

- a. Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited; and
- b. Reveal error messages only to organizational personnel with information security responsibilities.

Discussion: Organizations consider the structure and content of error messages. The extent to which systems can handle error conditions is guided and informed by organizational policy and operational requirements. Exploitable information includes stack traces and implementation details; erroneous logon attempts with passwords mistakenly entered as the username; mission or business information that can be derived from, if not stated explicitly by, the information recorded; and personally identifiable information, such as account numbers, social security numbers, and credit card numbers. Error messages may also provide a covert channel for transmitting information.

Related Controls: AU-2, AU-3, SI-2.

SI-12 INFORMATION MANAGEMENT AND RETENTION

[Existing] [Priority 3]

Control:

Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines and operational requirements.

Discussion: Information management and retention requirements cover the full life cycle of information, in some cases extending beyond system disposal. Information to be retained may also include policies, procedures, plans, reports, data output from control implementation, and other types of administrative information. The National Archives and Records Administration (NARA) provides federal policy and guidance on records retention and schedules. If organizations have a records management office, consider coordinating with records management personnel. Records produced from the output of implemented controls that may require management and retention include, but are not limited to: All XX-1, AC-6(9), AT-4,

AU-12, CA-2, CA-3, CA-5, CA-6, CA-7, CA-9, CM-2, CM-3, CM-4, CM-6, CM-8, CM-9, CM-12, CP-2, IR-6, IR-8, MA-2, MA-4, PE-2, PE-8, PE-16, PE-17, PL-2, PL-4, PL-8, PS-2, PS-6, PS-7, RA-2, RA-3, RA-5, SA-4, SA-5, SA-8, SA-10, SI-4, SR-2, SR-8.

Related Controls: AU-5, AU-11, CA-2, CA-3, CA-5, CA-6, CA-7, CA-9, CM-5, CM-9, CP-2, IR-8, MP-2, MP-3, MP-4, MP-6, PL-2, PL-4, PS-2, PS-6, RA-2, RA-3, SA-5, SA-8, SR-2.

Control Enhancements:

(1) INFORMATION MANAGEMENT AND RETENTION | LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS

[Existing] [Priority 3]

Control:

Limit personally identifiable information being processed in the information life cycle to the minimum PII necessary to achieve the purpose for which it is collected (see Section 4.3).

Discussion: Limiting the use of personally identifiable information throughout the information life cycle when the information is not needed for operational purposes helps to reduce the level of privacy risk created by a system. The information life cycle includes information creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposition. Risk assessments as well as applicable laws, regulations, and policies can provide useful inputs to determining which elements of personally identifiable information may create risk.

Related Controls: None.

(2) INFORMATION MANAGEMENT AND RETENTION | MINIMIZE PERSONALLY IDENTIFIABLE INFORMATION IN TESTING, TRAINING, AND RESEARCH

[Priority 3]

Control:

Use the following techniques to minimize the use of personally identifiable information for research, testing, or training: data obfuscation, randomization, anonymization, or use of synthetic data.

Discussion: Organizations can minimize the risk to an individual's privacy by employing techniques such as de-identification or synthetic data. Limiting the use of personally identifiable information throughout the information life cycle when the information is not needed for research, testing, or training helps reduce the level of privacy risk created by a system. Risk assessments as well as applicable laws, regulations, and policies can provide useful inputs to determining the techniques to use and when to use them.

Related Controls: None.

(3) INFORMATION MANAGEMENT AND RETENTION | INFORMATION DISPOSAL

[Existing] [Priority 3]

Control:

Use the following techniques to dispose of, destroy, or erase information following the retention period: as defined in MP-6.

Discussion: Organizations can minimize both security and privacy risks by disposing of information when it is no longer needed. The disposal or destruction of information applies to originals as well as copies and archived records, including system logs that may contain personally identifiable information.

Related Controls: MP-6.

SI-16 MEMORY PROTECTION

[Priority 2]

Control:

Implement the following controls to protect the system memory from unauthorized code execution: data execution prevention and address space layout randomization.

Discussion: Some adversaries launch attacks with the intent of executing code in nonexecutable regions of memory or in memory locations that are prohibited. Controls employed to protect memory include data execution prevention and address space layout randomization. Data execution prevention controls can either be hardware-enforced or software-enforced with hardware enforcement providing the greater strength of mechanism.

Related Controls: SI-7.

SUPPLY CHAIN RISK MANAGEMENT (SR)

SR-1 POLICY AND PROCEDURES

[Priority 2]

Control:

- a. Develop, document, and disseminate to organizational personnel with supply chain risk management responsibilities:
 1. Agency-level supply chain risk management policy that:
 - a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 - b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
 2. Procedures to facilitate the implementation of the supply chain risk management policy and the associated supply chain risk management controls;
- b. Designate organizational personnel with security responsibilities to manage the development, documentation, and dissemination of the supply chain risk management policy and procedures; and
- c. Review and update the current supply chain risk management:
 1. Policy annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI; and
 2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.

Discussion: Supply chain risk management policy and procedures address the controls in the SR family as well as supply chain-related controls in other families that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of supply chain risk management policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to supply chain risk management policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PS-8, SI-12.

Control Enhancements: None.

SR-2 SUPPLY CHAIN RISK MANAGEMENT PLAN

[Priority 3]

Control:

- a. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the following systems, system components or system services: systems used to process, store, or transmit CJI;
- b. Review and update the supply chain risk management plan annually or as required, to address threat, organizational or environmental changes; and
- c. Protect the supply chain risk management plan from unauthorized disclosure and modification.

Discussion: The dependence on products, systems, and services from external providers, as well as the nature of the relationships with those providers, present an increasing level of risk to an organization. Threat actions that may increase security or privacy risks include unauthorized production, the insertion or use of counterfeits, tampering, theft, insertion of malicious software and hardware, and poor manufacturing and development practices in the supply chain. Supply chain risks can be endemic or systemic within a system element or component, a system, an organization, a sector, or the Nation. Managing supply chain risk is a complex, multifaceted undertaking that requires a coordinated effort across an organization to build trust relationships and communicate with internal and external stakeholders.

Supply chain risk management (SCRM) activities include identifying and assessing risks, determining appropriate risk response actions, developing SCRM plans to document response actions, and monitoring performance against plans. The SCRM plan (at the system-level) is implementation specific, providing policy implementation, requirements, constraints and implications. It can either be stand-alone, or incorporated into system security and privacy plans. The SCRM plan addresses managing, implementation, and monitoring of SCRM controls and the development/sustainment of systems across the SDLC to support mission and business functions.

Because supply chains can differ significantly across and within organizations, SCRM plans are tailored to the individual program, organizational, and operational contexts. Tailored SCRM plans provide the basis for determining whether a technology, service, system component, or system is fit for purpose, and as such, the controls need to be tailored accordingly. Tailored SCRM plans help organizations focus their resources on the most critical mission and business functions based on mission and business requirements and their risk environment. Supply chain risk management plans include an expression of the supply chain risk tolerance for the organization, acceptable supply chain risk mitigation strategies or controls, a process for consistently evaluating and monitoring supply chain risk, approaches for implementing and communicating the plan, a description of and justification for supply chain risk mitigation

measures taken, and associated roles and responsibilities. Finally, supply chain risk management plans address requirements for developing trustworthy, secure, privacy-protective, and resilient system components and systems, including the application of the security design principles implemented as part of life cycle-based systems security engineering processes (see SA-8).

Related Controls: CA-2, CP-4, IR-4, MA-2, MA-6, PE-16, PL-2, RA-3, RA-7, SA-8, SI-4.

Control Enhancements:

(1) SUPPLY CHAIN RISK MANAGEMENT PLAN | ESTABLISH SCRM TEAM

[Priority 3]

Control:

Establish a supply chain risk management team consisting of individuals with security responsibilities and supply chain risk management responsibilities to lead and support the following SCRM activities: information technology, contracting, information security, privacy, mission or business, legal, supply chain and logistics, acquisition, business continuity, and other relevant functions.

Discussion: To implement supply chain risk management plans, organizations establish a coordinated, team-based approach to identify and assess supply chain risks and manage these risks by using programmatic and technical mitigation techniques. The team approach enables organizations to conduct an analysis of their supply chain, communicate with internal and external partners or stakeholders, and gain broad consensus regarding the appropriate resources for SCRM. The SCRM team consists of organizational personnel with diverse roles and responsibilities for leading and supporting SCRM activities, including risk executive, information technology, contracting, information security, privacy, mission or business, legal, supply chain and logistics, acquisition, business continuity, and other relevant functions. Members of the SCRM team are involved in various aspects of the SDLC and, collectively, have an awareness of and provide expertise in acquisition processes, legal practices, vulnerabilities, threats, and attack vectors, as well as an understanding of the technical aspects and dependencies of systems. The SCRM team can be an extension of the security and privacy risk management processes or be included as part of an organizational risk management team.

Related Controls: None.

SR-5 ACQUISITION STRATEGIES, TOOLS, AND METHODS

[Priority 2]

Control:

Employ the following acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks: use preferred suppliers who can provide attestation or demonstration of compliance with state or federal standards.

Discussion: The use of the acquisition process provides an important vehicle to protect the supply chain. There are many useful tools and techniques available, including obscuring the end use of a system or system component, using blind or filtered buys, requiring tamper-evident packaging, or using trusted or controlled distribution. The results from a supply chain risk assessment can guide and inform the strategies, tools, and methods that are most applicable to the situation. Tools and techniques may provide protections against unauthorized production, theft, tampering, insertion of counterfeits, insertion of malicious software or backdoors, and poor development practices throughout the system development life cycle. Organizations also consider providing incentives for suppliers who implement controls, promote transparency into their processes and security and privacy practices, provide contract language that addresses the prohibition of tainted or counterfeit components, and restrict purchases from untrustworthy suppliers. Organizations consider providing training, education, and awareness programs for personnel regarding supply chain risk, available mitigation strategies, and when the programs should be employed. Methods for reviewing and protecting development plans, documentation, and evidence are commensurate with the security and privacy requirements of the organization. Contracts may specify documentation protection requirements.

Related Controls: AT-3, SA-2, SA-3, SA-4, SA-5, SA-8, SA-9, SA-10, SA-15, SR-6, SR-10, SR-11.

SR-8 NOTIFICATION AGREEMENTS

[Priority 3]

Control:

Establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the notification of supply chain compromises to systems used to process, store, or transmit CJI.

Discussion: The establishment of agreements and procedures facilitates communications among supply chain entities. Early notification of compromises and potential compromises in the supply chain that can potentially adversely affect or have adversely affected organizational systems or system components is essential for organizations to effectively respond to such incidents. The results of assessments or audits may include open-source information that contributed to a decision or result and could be used to help the supply chain entity resolve a concern or improve its processes.

Related Controls: IR-4, IR-6, IR-8.

SR-10 INSPECTION OF SYSTEMS OR COMPONENTS

[Priority 3]

Control:

Inspect the following systems or system components upon initial procurement and periodically as needed to detect tampering: systems used to process, store, or transmit CJI.

Discussion: The inspection of systems or systems components for tamper resistance and detection addresses physical and logical tampering and is applied to systems and system components removed from organization-controlled areas. Indications of a need for inspection include changes in packaging, specifications, factory location, or entity in which the part is purchased, and when individuals return from travel to high-risk locations.

Related Controls: AT-3, SI-4, SI-7, SR-3, SR-5, SR-11.

SR-12 COMPONENT DISPOSAL

[Priority 3]

Control:

Dispose of CJI using the techniques and methods as described in Media Protection (MP).

Discussion: Data, documentation, tools, or system components can be disposed of at any time during the system development life cycle (not only in the disposal or retirement phase of the life cycle). For example, disposal can occur during research and development, design, prototyping, or operations/maintenance and include methods such as disk cleaning, removal of cryptographic keys, partial reuse of components.

Opportunities for compromise during disposal affect physical and logical data, including system documentation in paper-based or digital files; shipping and delivery documentation; memory sticks with software code; or complete routers or servers that include permanent media, which contain sensitive or proprietary information.

Additionally, proper disposal of system components helps to prevent such components from entering the gray market.

Related Controls: MP-6.

5.20 Policy Area 20: Mobile Devices

This policy area describes considerations and requirements for mobile devices including smartphones and tablets. Mobile devices are not limited to a single form factor or communications medium. The requirements in this section augment those in other areas of the Policy to address the gaps introduced by using mobile devices.

The agency shall: (i) establish usage restrictions and implementation guidance for mobile devices; and (ii) authorize, monitor, control wireless access to the information system. Wireless technologies, in the simplest sense, enable one or more devices to communicate without physical connections—without requiring network or peripheral cabling.

Appendix G provides reference material and additional information on mobile devices.

5.20.1 Wireless Communications Technologies

Examples of wireless communication technologies include, but are not limited to: 802.11, cellular, Bluetooth, satellite, microwave, and land mobile radio (LMR). Wireless technologies require at least the minimum security applied to wired technology and, based upon the specific technology or implementation, wireless technologies may require additional security controls as described below.

5.20.1.1 802.11 Wireless Protocols

Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) cryptographic algorithms, used by all pre-802.11i protocols, do not meet the requirements for FIPS 140-2 and shall not be used.

Agencies shall implement the following controls for all agency-managed wireless access points with access to an agency's network that processes unencrypted CJI:

1. Perform validation testing to ensure rogue APs (Access Points) do not exist in the 802.11 Wireless Local Area Network (WLAN) and to fully understand the wireless network security posture.
2. Maintain a complete inventory of all Access Points (APs) and 802.11 wireless devices.
3. Place APs in secured areas to prevent unauthorized physical access and user manipulation.
4. Test AP range boundaries to determine the precise extent of the wireless coverage and design the AP wireless coverage to limit the coverage area to only what is needed for operational purposes.
5. Enable user authentication and encryption mechanisms for the management interface of the AP.
6. Ensure that all APs have strong administrative passwords and ensure that all passwords are changed in accordance with Identification and Authentication (IA).
7. Ensure the reset function on APs is used only when needed and is only invoked by authorized personnel. Restore the APs to the latest security settings, when the reset functions are used, to ensure the factory default settings are not utilized.

8. Change the default service set identifier (SSID) in the APs. Disable the broadcast SSID feature so that the client SSID must match that of the AP. Validate that the SSID character string does not contain any agency identifiable information (division, department, street, etc.) or services.
9. Enable all security features of the wireless product, including the cryptographic authentication, firewall, and other available privacy features.
10. Ensure that encryption key sizes are at least 128-bits and the default shared keys are replaced by unique keys.
11. Ensure that the ad hoc mode has been disabled.
12. Disable all nonessential management protocols on the APs.
13. Ensure all management access and authentication occurs via FIPS compliant secure protocols (e.g., SFTP, HTTPS, SNMP over TLS, etc.). Disable non-FIPS compliant secure access to the management interface.
14. Enable logging (if supported) and review the logs on a recurring basis per local policy. At a minimum, logs shall be reviewed monthly.
15. Insulate, virtually (e.g., virtual local area network (VLAN) and ACLs) or physically (e.g., firewalls), the wireless network from the operational wired infrastructure. Limit access between wireless networks and the wired network to only operational needs.
16. When disposing of access points that will no longer be used by the agency, clear access point configuration to prevent disclosure of network configuration, keys, passwords, etc.

5.20.1.2 Cellular Devices

Cellular telephones, smartphones (i.e., Blackberry, iPhones, etc.), tablets, personal digital assistants (PDA), and “aircards” are examples of cellular handheld devices or devices that are capable of employing cellular technology. Additionally, cellular handheld devices typically include Bluetooth, infrared, and other wireless protocols capable of joining infrastructure networks or creating dynamic ad hoc networks.

Threats to cellular handheld devices stem mainly from their size, portability, and available wireless interfaces and associated services. Examples of threats to cellular handheld devices include:

1. Loss, theft, or disposal.
2. Unauthorized access.
3. Malware.
4. Spam.
5. Electronic eavesdropping.
6. Electronic tracking (threat to security of data and safety of the criminal justice professional).
7. Cloning (not as prevalent with later generation cellular technologies).
8. Server-resident data.

5.20.1.2.1 Cellular Service Abroad

Certain internal functions on cellular devices may be modified or compromised by the cellular carrier during international use as the devices are intended to have certain parameters configured by the cellular provider which is considered a “trusted” entity by the device.

When devices are authorized to access CJI outside the U.S., agencies shall perform an inspection to ensure that all controls are in place and functioning properly in accordance with the agency’s policies prior to and after deployment outside of the U.S.

5.20.1.2.2 Voice Transmissions Over Cellular Devices

Any cellular device used to transmit CJI via voice is exempt from the encryption and authentication requirements.

5.20.1.3 Bluetooth

Bluetooth is an open standard for short-range radio frequency (RF) communication. Bluetooth is used primarily to establish wireless personal area networks (WPAN). Bluetooth technology has been integrated into many types of business and consumer devices, including cell phones, laptops, automobiles, medical devices, printers, keyboards, mice, headsets, and biometric capture devices.

Bluetooth technology and associated devices are susceptible to general wireless networking threats (e.g., denial of service [DoS] attacks, eavesdropping, man-in-the-middle [MITM] attacks, message modification, and resource misappropriation) as well as specific Bluetooth-related attacks that target known vulnerabilities in Bluetooth implementations and specifications. Organizational security policy shall be used to dictate the use of Bluetooth and its associated devices based on the agency’s operational and business processes.

5.20.1.4 Mobile Hotspots

Many mobile devices include the capability to function as a Wi-Fi hotspot that allows other devices to connect through the device to the internet over the devices cellular network.

When an agency allows mobile devices that are approved to access or store CJI to function as a Wi-Fi hotspot connecting to the Internet, they shall be configured:

1. Enable encryption on the hotspot
2. Change the hotspot’s default SSID
 - a. Ensure the hotspot SSID does not identify the device make/model or agency ownership
3. Create a wireless network password (pre-shared key)
4. Enable the hotspot’s port filtering/blocking features if present
5. Only allow connections from agency-controlled devices

Note: Refer to the requirements in Systems and Communications Protection (SC) encryption for item #1. Refer to the requirements in Identification and Authentication (IA) for item #3.

OR

1. Have a MDM solution to provide the same security as identified in items 1 – 5 above.

5.20.2 Mobile Device Management (MDM)

Mobile Device Management (MDM) facilitates the implementation of sound security controls for mobile devices and allows for centralized oversight of configuration control, application usage, and device protection and recovery, if so desired by the agency.

Due to the potential for inconsistent network access or monitoring capability on mobile devices, methods used to monitor and manage the configuration of full-featured operating systems may not function properly on devices with limited-feature operating systems. MDM systems and applications coupled with device specific technical policy can provide a robust method for device configuration management if properly implemented.

Devices that have had any unauthorized changes made to them (including but not limited to being rooted or jailbroken) shall not be used to process, store, or transmit CJI data at any time. User agencies shall implement the following controls when directly accessing CJI from devices running a limited-feature operating system:

1. Ensure that CJI is only transferred between CJI authorized applications and storage areas of the device.
2. MDM with centralized administration configured and implemented to perform at least the following controls:
 - a. Remote locking of device
 - b. Remote wiping of device
 - c. Setting and locking device configuration
 - d. Detection of “rooted” and “jailbroken” devices
 - e. Enforcement of folder or disk level encryption
 - f. Application of mandatory policy settings on the device
 - g. Detection of unauthorized configurations
 - h. Detection of unauthorized software or applications
 - i. Ability to determine the location of agency-controlled devices
 - j. Prevention of unpatched devices from accessing CJI or CJI systems
 - k. Automatic device wiping after a specified number of failed access attempts

EXCEPTION: An MDM is not required when receiving CJI from an indirect access information system (i.e., the system provides no capability to conduct transactional activities on state and national repositories, applications or services). However, it is incumbent upon the authorized agency to ensure CJI is delivered to the appropriate requesting agency or individual. The CSO will make the final determination of whether access is considered indirect.

5.20.3 Wireless Device Risk Mitigations

Organizations shall, at a minimum, ensure that wireless devices:

1. Apply available critical patches and upgrades to the operating system as soon as they become available for the device and after necessary testing as described in System and Information Integrity (SI).
2. Are configured for local device authentication (see Section 5.20.7.1).

3. Use advanced authentication or CSO approved compensating controls as per Section 5.20.7.2.1.
4. Encrypt all CJI resident on the device.
5. Erase cached information, to include authenticators (see Identification and Authentication (IA)) in applications, when session is terminated.
6. Employ personal firewalls on full-featured operating system devices or run a Mobile Device Management (MDM) system that facilitates the ability to provide firewall services from the agency level.
7. Employ malicious code protection on full-featured operating system devices or run a MDM system that facilitates the ability to provide anti-malware services from the agency level.

5.20.4 System Integrity

Managing system integrity on limited function mobile operating systems may require methods and technologies significantly different from traditional full-featured operating systems. In many cases, the requirements of Section 5.10 of the CJIS Security Policy cannot be met with a mobile device without the installation of a third-party MDM, application, or supporting service infrastructure.

5.20.4.1 Patching/Updates

Based on the varying connection methods for mobile devices, an always on connection cannot be guaranteed for patching and updating. Devices without always-on cellular connections may not be reachable for extended periods of time by the MDM or solution either to report status or initiate patching.

Agencies shall monitor mobile devices to ensure their patch and update state is current.

5.20.4.2 Malicious Code Protection

Appropriately configured MDM software is capable of checking the installed applications on the device and reporting the software inventory to a central management console in a manner analogous to traditional virus scan detection of unauthorized software and can provide a high degree of confidence that only known software or applications are installed on the device.

Agencies that allow smartphones and tablets to access CJI shall have a process to approve the use of specific software or applications on the devices. Any device natively capable of performing these functions without a MDM solution is acceptable under this section.

5.20.4.3 Personal Firewall

For the purpose of this policy, a personal firewall is an application that controls network traffic to and from a user device, permitting or denying communications based on policy. A personal firewall shall be employed on all mobile devices that have a full-feature operating system (i.e., laptops or tablets with Windows or Linux/Unix operating systems). At a minimum, the personal firewall shall perform the following activities:

1. Manage program access to the Internet.
2. Block unsolicited requests to connect to the user device.

3. Filter incoming traffic by IP address or protocol.
4. Filter incoming traffic by destination ports.
5. Maintain an IP traffic log.

Mobile devices with limited-feature operating systems (i.e., tablets, smartphones) may not support a personal firewall. However, these operating systems have a limited number of system services installed, carefully controlled network access, and to a certain extent, perform functions similar to a personal firewall on a device with a full-feature operating system. Appropriately configured MDM software is capable of controlling which applications are allowed on the device.

5.20.5 Incident Response

In addition to the requirements in Section 5.3 Incident Response, agencies shall develop additional or enhanced incident reporting and handling procedures to address mobile device operating scenarios. Rapid response to mobile device related incidents can significantly mitigate the risks associated with illicit data access either on the device itself or within online data resources associated with the device through an application or specialized interface.

Special reporting procedures for mobile devices shall apply in any of the following situations:

1. Loss of device control. For example:
 - a. Device known to be locked, minimal duration of loss
 - b. Device lock state unknown, minimal duration of loss
 - c. Device lock state unknown, extended duration of loss
 - d. Device known to be unlocked, more than momentary duration of loss
2. Total loss of device
3. Device compromise
4. Device loss or compromise outside the United States

5.20.6 Access Control

Multiple user accounts are not generally supported on limited-feature mobile operating systems. Access control (Section 5.5 Access Control) shall be accomplished by the application that accesses CJI.

5.20.7 Identification and Authentication

Due to the technical methods used for identification and authentication on many limited-feature mobile operating systems, achieving compliance may require many different components.

5.20.7.1 Local Device Authentication

When mobile devices are authorized for use in accessing CJI, local device authentication shall be used to unlock the device for use. The authenticator used shall meet the requirements in Identification and Authentication (IA).

5.20.7.2 Advanced Authentication

When accessing CJI from an authorized mobile device, advanced authentication shall be used by the authorized user unless the access to CJI is indirect as described in Identification and Authentication (IA). If access is indirect, then AA is not required.

5.20.7.2.1 Compensating Controls

CSO approved compensating controls to meet the AA requirement on agency-issued smartphones and tablets with limited-feature operating systems are permitted. Compensating controls are temporary control measures that are implemented in lieu of the required AA control measures when an agency cannot meet a requirement due to legitimate technical or business constraints. Before CSOs consider approval of compensating controls, Mobile Device Management (MDM) shall be implemented per Section 5.20.2. The compensating controls shall:

1. Meet the intent of the CJIS Security Policy AA requirement
2. Provide a similar level of protection or security as the original AA requirement
3. Not rely upon the existing requirements for AA as compensating controls
4. Expire upon the CSO approved date or when a compliant AA solution is implemented.

Additionally, compensating controls may rely upon other, non-AA, existing requirements as compensating controls and/or be combined with new controls to create compensating controls.

The compensating controls for AA are a combination of controls providing acceptable assurance only the authorized user is authenticating and not an impersonator or (in the case of agency-issued device used by multiple users) controls that reduce the risk of exposure if information is accessed by an unauthorized party.

The following minimum controls shall be implemented as part of the CSO approved compensating controls:

- Possession and registration of an agency issued smartphone or tablet as an indication it is the authorized user
- Use of device certificates per Section 5.20.7.3 Device Certificates
- Implemented CJIS Security Policy compliant standard authenticator protection on the secure location where CJI is stored

5.20.7.3 Device Certificates

Device certificates are often used to uniquely identify mobile devices using part of a public key pair on the device in the form of a public key certificate. While there is value to ensuring the device itself can authenticate to a system supplying CJI, and may provide a critical layer of device identification or authentication in a larger scheme, a device certificate alone placed on the device shall not be considered valid proof that the device is being operated by an authorized user.

When certificates or cryptographic keys used to authenticate a mobile device are used in lieu of compensating controls for advanced authentication, they shall be:

1. Protected against being extracted from the device
2. Configured for remote wipe on demand or self-deletion based on a number of unsuccessful login or access attempts
3. Configured to use a secure authenticator (i.e., password, PIN) to unlock the key for use

APPENDICES

This policy area contains the various appendices. The appendices are:

- Appendix A—Terms and Definitions
- Appendix B—Acronyms
- Appendix C—Network Topology Diagrams
- Appendix D—Sample Information Exchange Agreements
- Appendix E—Security Forums and Organizational Entities
- Appendix F—Sample Forms
- Appendix G—Best Practices
- Appendix H—Security Addendum
- Appendix I—References

APPENDIX A: TERMS AND DEFINITIONS

28 CFR Certification Indicator — True if the user has been trained and certified in the handling of criminal intelligence data in accordance with Code of Federal Regulations Title 28 (28 CFR) Part 23, false otherwise. Usage information: Assertion of this privilege requires the user to have been trained and certified in the handling of criminal intelligence data in accordance with Code of Federal Regulations Title 28 (28 CFR) Part 23. One way for a user to meet this requirement is by having taken and passed the online 28 CFR Part 23 training course and certification exam offered by the U.S. Department of Justice Bureau of Justice Assistance (BJA) via its Secured National Criminal Intelligence Resource Center (NCIRC) Web Site (<http://www.ncirc.gov/securedwebsite.cfm>). Alternatively, a user may meet this requirement by having taken and passed an equivalent offline 28 CFR Part 23 training course, offered by the Institute for Intergovernmental Research (IIR). (See <https://28cfr.iir.com/> for details.)

Access to Criminal Justice Information — The physical or logical (electronic) ability, right or privilege to view, modify or make use of Criminal Justice Information.

Administration of Criminal Justice — The detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. It also includes criminal identification activities; the collection, storage, and dissemination of criminal history record information; and criminal justice employment. In addition, administration of criminal justice includes “crime prevention programs” to the extent access to criminal history record information is limited to law enforcement agencies for law enforcement programs (e.g., record checks of individuals who participate in Neighborhood Watch or “safe house” programs) and the result of such checks will not be disseminated outside the law enforcement agency.

Agency Controlled Mobile Device — A mobile device that is centrally managed by an agency for the purpose of securing the device for potential access to CJI. The device can be agency issued or BYOD (personally owned).

Agency Coordinator (AC) — A staff member of the Contracting Government Agency who manages the agreement between the Contractor and agency.

Agency Issued Mobile Device — A mobile device that is owned by an agency and issued to an individual for use. It is centrally managed by the agency for the purpose of securing the device for potential access to CJI. The device is not BYOD (personally owned).

Agency Liaison (AL) — Coordinator of activities between the criminal justice agency and the noncriminal justice agency when responsibility for a criminal justice system has been delegated by a criminal justice agency to a noncriminal justice agency, which has in turn entered into an agreement with a contractor. The agency liaison shall, inter alia, monitor compliance with system security requirements. In instances in which the noncriminal justice agency’s authority is directly from the CJIS systems agency, there is no requirement for the appointment of an agency liaison.

Asymmetric Encryption — A type of encryption that uses key pairs for encryption. One key is used to encrypt a message and another key to decrypt the message. Asymmetric encryption is also commonly known as public key encryption.

Authenticator Assurance Level — The authenticator assurance level as defined by NIST SP 800-63-3. There are three defined levels: AAL1 (low), AAL2 (medium), and AAL3 (high). Usage

information: IDPs should assert this attribute to indicate the strength of the authenticator used for the current authentication process; AAL1 (low), AAL2 (medium), and AAL3 (high). AAL2 and AAL3 require multifactor authentication; although the use of multiple factors does not automatically qualify for AAL2.

Authorized User/Personnel — An individual, or group of individuals, who have been appropriately vetted through a national fingerprint-based record check and have been granted access to CJI.

Authorized Recipient (AR) — (1) A criminal justice agency or federal agency authorized to receive CHRI pursuant to federal statute or executive order; (2) A nongovernmental entity authorized by federal statute or executive order to receive CHRI for noncriminal justice purposes; or (3) A government agency authorized by federal statute or executive order, or state statute which has been approved by the United States Attorney General to receive CHRI for noncriminal justice purposes.

Authorized Recipient Security Officer (ARSO) — the individual appointed by the AR to coordinate and oversee Information Security by ensuring that the Channeler is adhering to the CJISSECPOL and Outsourcing Standard, verifying the completion of annual Security Awareness Training, and communicating with the FBI CJIS Division on matters relating to Information Security.

Availability — The degree to which information, a system, subsystem, or equipment is operable and in a useable state; frequently represented as a proportion of time the element is in a functioning condition.

Basic Testing — A test methodology that assumes no knowledge of the internal structure and implementation detail of the assessment object. Also known as black box testing.

Comprehensive Testing — A test methodology that assumes explicit and substantial knowledge of the internal structure and implementation detail of the assessment object. Also known as white box testing.

Biographic Data — Information collected about individuals associated with a unique case, and not necessarily connected to identity data. Biographic Data does not provide a history of an individual, only information related to a unique case.

Biometric Data — When applied to CJI, it is used to identify individuals, and includes the following types: fingerprints, palm prints, DNA, iris, and facial recognition.

Case / Incident History — All relevant information gathered about an individual, organization, incident, or combination thereof, arranged so as to serve as an organized record to provide analytic value for a criminal justice organization. In regards to CJI, it is the information about the history of criminal incidents.

Certificate Authority (CA) Certificate — Digital certificates required for certificate-based authentication that are issued to tell the client computers and servers that it can trust other certificates that are issued by this CA.

Channeler — A FBI approved contractor, who has entered into an agreement with an Authorized Recipient(s), to receive noncriminal justice applicant fingerprint submissions and collect the associated fees. The Channeler ensures fingerprint submissions are properly and adequately

completed, electronically forwards fingerprint submissions to the FBI's CJIS Division for national noncriminal justice criminal history record check, and receives electronic record check results for dissemination to Authorized Recipients. A Channeler is essentially an "expediter" rather than a user of criminal history record check results.

Cloud Client — A machine or software application that accesses cloud services over a network connection, perhaps on behalf of a subscriber.

Cloud Computing — A distributed computing model that permits on-demand network access to a shared pool of configurable computing resources (i.e., networks, servers, storage, applications, and services), software, and information.

Cloud Provider — An organization that provides cloud computing services.

Cloud Subscriber — A person or organization that is a customer of a cloud computing service provider.

CJIS Advisory Policy Board (APB) — The governing organization within the FBI CJIS Advisory Process composed of representatives from criminal justice and national security agencies within the United States. The APB reviews policy, technical, and operational issues relative to CJIS Division programs and makes subsequent recommendations to the Director of the FBI.

CJIS Audit Unit (CAU) — The organization within the FBI CJIS Division responsible to perform audits of CSAs to verify compliance with the CJIS Security Policy.

CJIS Security Policy — The FBI CJIS Security Policy document as published by the FBI CJIS ISO; the document containing this glossary.

CJIS Systems Agency (CSA) — A duly authorized state, federal, international, tribal, or territorial criminal justice agency on the CJIS network providing statewide (or equivalent) service to its criminal justice users with respect to the CJI from various systems managed by the FBI CJIS Division. There shall be only one CSA per state or territory. In federal agencies, the CSA may be the interface or switch to other federal agencies connecting to the FBI CJIS systems.

CJIS Systems Agency Information Security Officer (CSA ISO) — The appointed FBI CJIS Division personnel responsible to coordinate information security efforts at all CJIS interface agencies.

CJIS Systems Officer (CSO) — The individual located within the CJIS Systems Agency responsible for the administration of the CJIS network on behalf of the CJIS Systems Agency.

Compact Council — The entity created by the National Crime Prevention and Privacy Compact of 1998 that has the authority to promulgate rules and procedures governing the use of the III system for noncriminal justice purposes.

Compact Officers — The leadership of the Compact Council, oversees the infrastructure established by the National Crime Prevention and Privacy Compact Act of 1998, which is used by ratifying states to exchange criminal records for noncriminal justice purposes. Their primary responsibilities are to promulgate rules and procedures for the effective and appropriate use of the III system.

Compensating Controls — Compensating controls are temporary control measures implemented in lieu of the required control measures when an agency cannot meet the AA requirement due to legitimate technical or business constraints. The compensating controls must:

1. Meet the intent of the CJIS Security Policy AA requirement
2. Provide a similar level of protection or security as the original AA requirement
3. Not rely upon the existing requirements for AA as compensating controls

Additionally, compensating controls may rely upon other, non-AA, existing requirements as compensating controls and/or be combined with new controls to create compensating controls.

Computer Security Incident Response Capability (CSIRC) — A collection of personnel, systems, and processes that are used to efficiently and quickly manage a centralized response to any sort of computer security incident which may occur.

Confidentiality — The concept of ensuring that information is observable only to those who have been granted authorization to do so.

Contractor — A private business, agency or individual which has entered into an agreement for the administration of criminal justice or noncriminal justice functions with a Criminal Justice Agency or a Noncriminal Justice Agency. Also, a private business approved by the FBI CJIS Division to contract with Noncriminal Justice Agencies to perform noncriminal justice functions associated with civil fingerprint submission for hiring purposes.

Contracting Government Agency (CGA) — The government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor.

Controlled Unclassified Information (CUI) — Information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. (32 CFR Vol 6 Part 2002)

Counter Terrorism Data Self Search Home Privilege Indicator — True if the user has permission to search on behalf of himself/herself (NOT on behalf of the user's home agency) for counter-terrorism data and documents within the user's home system, network, or agency. False otherwise. Usage information: Legal values for this attribute are "true", "false", "1", and "0", where "1" indicates true and "0" indicates false.

Crime Reports Data — The data collected through the Uniform Crime Reporting program and reported upon annually by the FBI CJIS division used to analyze the crime statistics for the United States.

Criminal History Data Self Search Home Privilege Indicator — True if the user has permission to search on behalf of himself/herself (NOT on behalf of the user's home agency) for criminal history data and documents within the user's home system, network, or agency. False otherwise. Usage information: Example data sources include National Crime Information Center (NCIC) Criminal History. User eligibility requirements are decided by federation members, but may include: Fingerprint (FP) based background, NCIC training, access to Law Enforcement criminal history data in home agency, member of agency with Law Enforcement Originating Agency (ORI) code. Legal values for this attribute are "true", "false", "1", and "0", where "1" indicates true and "0" indicates false.

Criminal History Record Information (CHRI) — Information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions,

indictments, informations, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, and release. The term does not include identification information such as fingerprint records if such information does not indicate the individual's involvement with the criminal justice system.

Criminal Intelligence Data Self Search Home Privilege Indicator — True if the user has permission to search on behalf of himself/herself (NOT on behalf of the user's home agency) for criminal intelligence data and documents within the user's home system, network, or agency. False otherwise. Usage information: Example data sources include Criminal Law Enforcement Reporting Information System (CLERIS), Regional Information Sharing Systems (RISS), Joint Regional Information Exchange System (JRIES), and Law Enforcement Intelligence Units (LEIU). User eligibility requirements are decided by federation members, but may include: 28 CFR (23) training, Fingerprint (FP) based background, access to intelligence data in home agency, member of agency with Law Enforcement Originating Agency (ORI) code. Legal values for this attribute are "true", "false", "1", and "0", where "1" indicates true and "0" indicates false.

Criminal Investigative Data Self Search Home Privilege Indicator — True if the user has permission to search on behalf of himself/herself (NOT on behalf of the user's home agency) for criminal investigative data and documents within the user's home system, network, or agency. False otherwise. Usage information: Example data sources include Criminal Law Enforcement Reporting Information System (CLERIS) and Contact and Information Management System (CIMS). User eligibility requirements are decided by federation members, but may include: Fingerprint (FP) based background, access to investigative data in home agency, member of agency with Law Enforcement Originating Agency (ORI) code. Legal values for this attribute are "true", "false", "1", and "0", where "1" indicates true and "0" indicates false.

Criminal Justice Agency (CJA) — The courts, a governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspectors General Offices are included.

Criminal Justice Agency User Agreement — A terms-of-service agreement that must be signed prior to accessing CJI. This agreement is required by each CJA and spells out user's responsibilities, the forms and methods of acceptable use, penalties for their violation, disclaimers, and so on.

Criminal Justice Conveyance — A criminal justice conveyance is any enclosed mobile vehicle used for the purposes of criminal justice activities with the capability to comply, during operational periods, with the requirements of Section 5.9.1.3.

Criminal Justice Information (CJI) — Criminal Justice Information is the abstract term used to refer to all of the FBI CJIS provided data necessary for law enforcement agencies to perform their mission and enforce the laws, including but not limited to: biometric, identity history, person, organization, property (when accompanied by any personally identifiable information), and case/incident history data. In addition, CJI refers to the FBI CJIS-provided data necessary for civil agencies to perform their mission; including, but not limited to data used to make hiring decisions. The following type of data are exempt from the protection levels required for CJI: transaction control type numbers (e.g., ORI, NIC, UCN, etc.) when not accompanied by information that reveals CJI or PII.

Criminal Justice Information Services Division (FBI CJIS or CJIS) — The FBI division responsible for the collection, warehousing, and timely dissemination of relevant CJI to the FBI and to qualified law enforcement, criminal justice, civilian, academic, employment, and licensing agencies.

Data — See Information and CJI.

Data Center — A physical room, building, or facility housing Information Technology infrastructure for developing, running, and delivering applications and services associated with storing and managing data, as determined by the CSO, his/her designee, or Interface Agency Official.

Decryption — The inverse cryptographic operation used to convert encrypted information back into a plaintext (readable) format.

Degauss — Neutralize a magnetic field to erase information from a magnetic disk or other storage device. In the field of information technology, degauss has become synonymous with erasing information whether or not the medium is magnetic. In the event the device to be degaussed is not magnetic (e.g., solid state drive, USB storage device), steps other than magnetic degaussing may be required to render the information irretrievable from the device.

Department of Justice (DoJ) — The Department within the U.S. Government responsible to enforce the law and defend the interests of the United States according to the law, to ensure public safety against threats foreign and domestic, to provide federal leadership in preventing and controlling crime, to seek just punishment for those guilty of unlawful behavior, and to ensure fair and impartial administration of justice for all Americans.

Digital Media — Any form of electronic media designed to store data in a digital format. This includes, but is not limited to: memory device in laptops, computers, and mobile devices; and any removable, transportable electronic media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card.

Digital Signature — A digital signature consists of three algorithms: (1) A key generation algorithm that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key. (2) A signing algorithm that, given a message and a private key, produces a signature. (3) A signature verifying algorithm that, given a message, public key, and a signature, either accepts or rejects the message's claim to authenticity. Two main properties are required. First, a signature generated from a fixed message and fixed private key should verify the authenticity of that message by using the corresponding public key. Secondly, it should be computationally infeasible to generate a valid signature for a party who does not possess the private key.

Direct Access — (1) Having the authority to access systems managed by the FBI CJIS Division, whether by manual or automated methods, not requiring the assistance of, or intervention by, any other party or agency (28 CFR, Chapter 1, Part 20). (2) Having the authority to query or update national databases maintained by the FBI CJIS Division including national queries and updates automatically or manually generated by the CSA.

Display Name — The user's display name is a text string formatted for display purposes in applications and correspondence.

Dissemination — The transmission/distribution of CJI to Authorized Recipients within an agency.

Email Address Text — The electronic mailing address by which the user may be contacted.

Employer Name — The name of the organization that is the user's primary employer.

Employer ORI — A unique identifier assigned to the organization that is the user's primary employer. ORIs are generally assigned by the FBI; however, in some cases they may be assigned by other agencies.

Employer Organization General Category Code — The general category of the organization that is the user's primary employer.

Employer State Code — The state, commonwealth, province, or other such geopolitical subdivision of the country in which is located the primary business office of the organization that is the user's primary employer.

Encryption — A form of cryptology that applies a cryptographic operation to provide confidentiality of (sensitive) information.

Escort — Authorized personnel who accompany a visitor at all times while within a physically secure location to ensure the protection and integrity of the physically secure location and any Criminal Justice Information therein. The use of cameras or other electronic means used to monitor a physically secure location does not constitute an escort.

Facsimile (Fax) — Facsimile is: (a) a document received and printed on a single or multi-function stand-alone device, (b) a single or multi-function stand-alone device for the express purpose of transmitting and receiving documents from a like device over a standard telephone line, or (c) a facsimile server, application, service which implements email-like technology and transfers documents over a network.

Federal Bureau of Investigation (FBI) — The agency within the DOJ responsible to protect and defend the United States against terrorist and foreign intelligence threats, to uphold and enforce the criminal laws of the United States, and to provide leadership and criminal justice services to federal, state, municipal, and international agencies and partners.

FBI CJIS Information Security Officer (FBI CJIS ISO) — The FBI personnel responsible for the maintenance and dissemination of the FBI CJIS Security Policy; the liaison between the FBI and the CSA's ISOs and other relevant security points-of-contact (POCs); the provider of technical guidance as to the intent and implementation of technical policy issues; the POC for computer incident notification which also disseminates security alerts to the CSOs and ISOs.

Federal Information Security Management Act (FISMA) — The Federal Information Security Management Act of 2002, a US Federal law that established information security standards for the protection of economic and national security interests of the United States. It requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

Federation Assurance Level — There are 3 Federation Assurance Levels representing the assurance level of the user's federated assertion: FAL1 (low assurance), FAL2 (moderate assurance), and FAL3 (high assurance) based on NIST SP 800-63-3. Usage information: IDPs

should assert this for all assertions sent to RPs correctly identifying the level of assurance of the assertion. The RP can also derive the FAL if not asserted.

Federation Id — The persistent, federation-unique identifier for the user, comprising a federation part, an optional trusted identity broker (TIB) part, an identity provider (IDP) part, and a local ID.

Focused Testing — A test methodology that assumes some knowledge of the internal structure and implementation detail of the assessment object. Also known as gray box testing.

For Official Use Only (FOUO) — A caveat applied to unclassified sensitive information that may be exempt from mandatory release to the public under the Freedom of Information Act (FOIA), 5 U.S.C 522. In general, information marked FOUO shall not be disclosed to anybody except Government (Federal, State, tribal, or local) employees or contractors with a need to know.

Full-feature Operating System — Full-feature operating systems are traditional operating systems used by a standard desktop computer (e.g., Microsoft Windows, Apple OSX/macOS, LINUX/UNIX, etc.). These operating systems are generally open to user control and configuration and therefore require configuration management to properly secure, or “harden”, these devices from malicious network based technical attacks (e.g., malware, spyware, hackers, etc.). These operating systems require traditional protection applications such as antivirus programs and personal firewalls.

General User — A user, but not a process, who is authorized to use an information system.

Given Name — The first name of the user.

Government Data Self Search Home Privilege Indicator — True if the user has permission to search on behalf of himself/herself (NOT on behalf of the user's home agency) for government data and documents within the user's home system, network, or agency. False otherwise. Usage information: Example data sources include Tax Data, Labor Data, Uniform Commercial Code (UCC) Filings, Property Records, Department of Motor Vehicles (DMV), Drivers License (DL), Boat Ownership, Corporate Records, and Protected Critical Infrastructure Information (PCII). User eligibility requirements are decided by federation members, but may include: Agency vetting, application training, state law, and Federal law. Legal values for this attribute are "true", "false", "1", and "0", where "1" indicates true and "0" indicates false.

Guest Operating System — An operating system that has emulated hardware presented to it by a host operating system. Also referred to as the virtual machine (VM).

Hashing — The process of applying a mathematical algorithm to data to produce an alphanumeric value (i.e., hash value) to be used as a representative of that data.

Hash Value — The term that refers to an alphanumeric value which represents the result of applying a cryptographic hash function to data.

Host Operating System — In the context of virtualization, the operating system that interfaces with the actual physical hardware and arbitrates between it and the guest operating systems. It is also referred to as a hypervisor.

Hybrid Encryption — A type of encryption where both asymmetric encryption and symmetric encryption keys are used creating what is referred to as cipher suites. In a hybrid solution, the asymmetric encryption keys are used for client/server certificate exchange to provide session

integrity while the symmetric encryption keys are used for bulk data encryption to provide data confidentiality.

Hypervisor — See Host Operating System.

Identity Assurance Level — The maximum NIST identity assurance level as defined by NIST SP 800-63-3 for which the identity proofing process of this Identity Provider Organization qualifies. There are three defined levels: IAL1 (low), IAL2 (medium), and IAL3 (high). Usage information: IDPs should use this attribute to indicate the assurance level of their identity and attribute proofing processes.

Identity History Data — Textual data that corresponds with an individual's biometric data, providing a history of criminal and/or civil events for the identified individual.

Identity Provider Id — The unique identifier within the federation that identifies the identity provider (IDP) of the user within the federation. Comprises a federation part, an optional trusted identity broker (TIB) part, and an identity provider (IDP) part. The general format of an identity provider ID is: "{Federation}:{TIB:{TIB}}:IDP:{IDP}". Usage information: This identifier MUST be consistent with the federation identifier, IDP identifier, and (if applicable) TIB identifier denoted within the user's Federation Id attribute.

In-Band — The communication service channel (network connection, email, SMS text, phone call, etc.) used to obtain an authenticator is the same as the one used for login.

Indirect Access — Having the authority to access systems containing CJI without providing the user the ability to conduct transactional activities (the capability to query or update) on state and national systems (e.g., CJIS Systems Agency (CSA), State Identification Bureau (SIB), or national repositories).

Information — See data and CJI.

Information Exchange Agreement — An agreement that codifies the rules by which two parties engage in the sharing of information. These agreements typically include language which establishes some general duty-of-care over the other party's information, whether and how it can be further disseminated, penalties for violations, the laws governing the agreement (which establishes venue), procedures for the handling of shared information at the termination of the agreement, and so on. This document will ensure consistency with applicable federal laws, directives, policies, regulations, standards and guidance.

Information Security Officer (ISO) — Typically a member of an organization who has the responsibility to establish and maintain information security policy, assesses threats and vulnerabilities, performs risk and control assessments, oversees the governance of security operations, and establishes information security training and awareness programs. The ISO also usually interfaces with security operations to manage implementation details and with auditors to verify compliance to established policies.

Information System — A system of people, data, and processes, whether manual or automated, established for the purpose of managing information.

Integrated Automated Fingerprint Identification System (IAFIS) — The national fingerprint and criminal history system maintained by the FBI CJIS Division that provides the law

enforcement community with automated fingerprint search capabilities, latent searching capability, electronic image storage, and electronic exchange of fingerprints and responses.

Integrity — The perceived consistency of expected outcomes, actions, values, and methods of an individual or organization. As it relates to data, it is the concept that data is preserved in a consistent and correct state for its intended use.

Intelligence Analyst Indicator — True if the user is an Intelligence Analyst (IA) for a government agency, false otherwise. Usage information: An Identity Provider (IdP) may assert that a user is an IA if they work for a government agency, and/or company who works with the government, in order to provide information assessments about criminal or security threats.

Interconnection Security Agreement (ISA) — An agreement much like an Information Exchange Agreement as mentioned above, but concentrating more on formalizing the technical and security requirements pertaining to some sort of interface between the parties' information systems.

Interface Agency — A criminal justice agency (including law enforcement) or any federally authorized agency/entity, other than a CSA or State Identification Bureau (SIB), that leverages a direct connection to the FBI CJIS Division.

Internet Protocol (IP) — A protocol used for communicating data across a packet-switched internetwork using the Internet Protocol Suite, also referred to as TCP/IP. IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses.

Interstate Identification Index (III) — The CJIS service that manages automated submission and requests for CHRI that is warehoused subsequent to the submission of fingerprint information. Subsequent requests are directed to the originating State as needed.

Intrusion Detection — The process of monitoring the events occurring in an information system or network and analyzing them for signs of possible incidents.

Intrusion Detection System — Software which automates the intrusion detection process.

Intrusion Prevention — The process of monitoring events occurring in an information system or network and analyzing them for signs of possible incidents and attempting to stop detected possible incidents.

Intrusion Prevention System — Software which has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents.

Jailbreak (Jailbroken) — The process of attaining privileged control (known as “root access”) of a device running the Apple iOS operating system that ultimately allows a user the ability to alter or replace system applications and settings, run specialized applications that require administrator-level permissions, or perform other operations that are otherwise not allowed.

Laptop Devices — Laptop devices are mobile devices with a full-featured operating system (e.g., Microsoft Windows, Apple OSX/macOS, LINUX/UNIX, etc.). Laptops are typically intended for transport via vehicle mount or portfolio-sized carry case, but not on the body. This definition does not include pocket/handheld devices (e.g., smartphones), or mobile devices that feature a limited-feature operating system (e.g., tablets).

Law Enforcement Enterprise Portal (LEEP) — A secure, Internet-based communications portal provided by the FBI CJIS Division for use by law enforcement, first responders, criminal justice professionals, and anti-terrorism and intelligence agencies around the globe. Its primary purpose is to provide a platform on which various law enforcement agencies can collaborate on FOUO matters.

Limited-feature Operating System — Limited-feature operating systems are designed specifically for the mobile environment where battery life and power efficiency are primary design drivers (e.g., Apple iOS, Android, Windows Mobile, Blackberry OS, etc.). These operating systems permit limited user control, but are inherently more resistant than a full-feature operating system to certain types of network based technical attacks due to the limited-feature sets. Devices using these operating systems are required to be managed by a mobile device management solution.

Local Id — The unique local identifier associated with the user for internal purposes within the user's identity provider (IDP). This identifier is assigned and maintained by a federation member agency or partner organization and used for local authentication and identification. The identifier typically has local significance and is integrated into the existing legacy IT infrastructure and/or business processes of the federation member agency or partner organization.

Logical Access — The technical means (e.g., read, create, modify, delete a file, execute a program, or use an external connection) for an individual or other computer system to utilize CJI or CJIS applications.

Logical Partitioning — When the host operating system, or hypervisor, allows multiple guest operating systems to share the same physical resources.

Local Agency Security Officer (LASO) — The primary Information Security contact between a local law enforcement agency and the CSA under which this agency interfaces with the FBI CJIS Division. The LASO actively represents their agency in all matters pertaining to Information Security, disseminates Information Security alerts and other material to their constituents, maintains Information Security documentation (including system configuration data), assists with Information Security audits of hardware and procedures, and keeps the CSA informed as to any Information Security needs and problems.

Management Control Agreement (MCA) — An agreement between parties that wish to share or pool resources that codifies precisely who has administrative control over, versus overall management and legal responsibility for, assets covered under the agreement. An MCA must ensure the CJA's authority remains with regard to all aspects of Section 3.2.2. The MCA usually results in the CJA having ultimate authority over the CJI supporting infrastructure administered by the NCJA.

Metadata — Structured information that describes, explains, locates or otherwise makes it easier to retrieve, use or manage an information resource. Metadata is commonly referred to as data about data, information about information, or information describing the characteristics of data.

Mobile Device — Any portable device used to access CJI via a wireless connection (e.g., cellular, Wi-Fi, Bluetooth, etc.).

Mobile Device Management (MDM) — Centralized administration and control of mobile devices specifically including, but not limited to, cellular phones, smart phones, and tablets.

Management typically includes the ability to configure device settings and prevent a user from changing them, remotely locating a device in the event of theft or loss, and remotely locking or wiping a device. Management can also include over-the-air distribution of applications and updating installed applications.

Mobile (Wi-Fi) Hotspot — A mobile (Wi-Fi) hotspot is a zone or area associated with a mobile device (e.g., smartphone, air card) allowing wireless connectivity to the Internet typically through a cellular connection.

National Crime Information Center (NCIC) — An information system which stores CJI which can be queried by appropriate Federal, state, and local law enforcement and other criminal justice agencies.

National Instant Criminal Background Check System (NICS) — A system mandated by the Brady Handgun Violence Prevention Act of 1993 that is used by Federal Firearms Licensees (FFLs) to instantly determine via telephone or other electronic means whether the transfer of a firearm would be in violation of Section 922 (g) or (n) of Title 18, United States Code, or state law, by evaluating the prospective buyer's criminal history.

National Institute of Standards and Technology (NIST) — Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Department of Commerce whose mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic and national security.

Noncriminal Justice Agency (NCJA) — A governmental agency, or any subunit thereof, that provides services primarily for purposes other than the administration of criminal justice. Examples of services include, but not limited to, employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

NCJA (Government) — A Federal, state, local, or tribal governmental agency or any subunit thereof whose charter does not include the responsibility to administer criminal justice, but may have a need to process CJI. An example would be the central IT organization within a state government that administers equipment on behalf of a state law-enforcement agency.

NCJA (Private) — A private agency or subunit thereof whose charter does not include the responsibility to administer criminal justice, but may have a need to process CJI. An example would include a local bank.

NCJA (Public) — A public agency or sub-unit thereof whose charter does not include the responsibility to administer criminal justice, but may have a need to process CJI. An example would include a county school board which uses CHRI to assist in employee hiring decisions.

NCIC Certification Indicator — True if the user has a valid, active certification in the usage and handling of data in accordance with National Crime Information Center (NCIC) rules and regulations, false otherwise.

N-DEx Privilege Indicator — True if the user has privileges to access the Federal Bureau of Investigation (FBI) Law Enforcement National Data Exchange (N-DEx), false otherwise. Usage information: Assertion of this privilege requires the user to meet certain requirements which are not currently documented in the GFIPM Metadata Specification. Future versions of this spec will properly document these requirements. Legal values for this attribute are "true", "false", "1", and "0", where "1" indicates true and "0" indicates false.

Noncriminal Justice Purpose — The uses of criminal history records for purposes authorized by federal or state law other than purposes relating to the administration of criminal justice, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

Non-digital Media — Non-digital media means a hard copy or physical representation of information, including, but not limited to, paper copies, printer ribbons, drums, microfilm, platens, and other forms of preserved or preservable information.

Office of Management and Budget (OMB) — The agency within the Executive Branch of the Federal government responsible to oversee the preparation of the federal budget, to assist in the supervision of other Executive Branch agencies, and to oversee and coordinate the Presidential Administration's procurement, financial management, information, and regulatory policies.

One-time Password — A disposable, single-use standard authenticator for access CJI. One-time passwords are: minimum of six (6) randomly generated characters, valid for a single session, and if not used, expire within a minimum of five (5) minutes after issuance.

Organizational Personnel with Security Responsibilities — Personnel with the responsibility to ensure the confidentiality, integrity, and availability of CJI and the implementation of technology in a manner compliant with the CJISSECPOL.

Out-of-Band — The communication service channel (network connection, email, SMS text, phone call, etc.) used to obtain an authenticator is separate from that used for login.

Outsourcing — The process of delegating in-house operations to a third-party. For instance, when the administration of criminal justice functions (network operations, dispatch functions, system administration operations, etc.) are performed for the criminal justice agency by a city or county information technology department or are contracted to be performed by a vendor.

Outsourcing Standard — National Crime Prevention and Privacy Compact Council's Outsourcing Standard. The Compact Council's uniform standards and processes for the interstate and Federal-State exchange of criminal history records for noncriminal justice purposes.

Partitioning — Managing guest operating system, or virtual machine, access to hardware so that each guest OS can access its own resources but cannot encroach on the other guest operating systems resources or any resources not allocated for virtualization use.

Password Verifier (Verifier) — An entity or process that verifies the claimant's identity by verifying the claimant's possession and control of one or two authenticators using an authentication protocol. To do this, the Verifier may also need to validate credentials that link the authenticator(s) to the subscriber's identifier and check their status.

PCII Certification Indicator — True if the user has a valid, active certification in the usage and handling of Protected Critical Infrastructure Information (PCII) data in accordance with US Department of Homeland Security (DHS) rules and regulations, false otherwise. Usage information: Information about PCII authorized user training is available at the following URL. <http://www.dhs.gov/receive-pcii-authorized-user-training>

Personal Firewall — An application which controls network traffic to and from a computer, permitting or denying communications based on a security policy.

Personally Identifiable Information (PII) — PII is information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name.

Physical Access — The physical ability, right or privilege to view, modify or make use of Criminal Justice Information (CJI) by means of physical presence within the proximity of computers and network devices (e.g., the ability to insert a boot disk or other device into the system, make a physical connection with electronic equipment, etc.).

Physical Media — Physical media refers to media in printed form. This definition includes, but is not limited to, printed documents, printed imagery, printed facsimile.

Physical Partitioning — When the host operating system, or hypervisor, assigns separate physical resources to each guest operating systems, or virtual machine.

Physically Secure Location — A facility, a criminal justice conveyance, or an area, a room, or a group of rooms, within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems.

Pocket/Handheld Mobile Device — Pocket/Handheld mobile devices (e.g., smartphones) are intended to be carried in a pocket or holster attached to the body and feature an operating system with limited functionality (e.g., iOS, Android, BlackBerry, etc.). This definition does not include tablet and laptop devices.

Privileged User — A user that is authorized (and, therefore, trusted) to perform security-relevant functions that general users are not authorized to perform.

Property Data — Information about vehicles and property associated with a crime.

Public Safety Officer Indicator — True if the user is a public safety officer (PSO), false otherwise. Usage information: An IDP may assert that a user is a PSO if the user is authorized to act in a role pursuant to the safety and welfare of the public within a government jurisdiction. This may include firefighters, emergency medical technicians (EMTs), hazardous materials (HAZMAT) cleanup specialists, etc.

Rap Back — A NGI service that allows authorized agencies to receive notification of subsequent criminal activity reported to the FBI committed by persons of interest.

Receive-Only Terminal (ROT) — A device that is configured to accept a limited type of data but is technically prohibited from forming or transmitting data, browsing or navigating internal or external networks, or otherwise performing outside the scope of receive only (e.g., a printer, dumb terminal, etc.).

Repository Manager, or Chief Administrator — The designated manager of the agency having oversight responsibility for a CSA's fingerprint identification services. If both state fingerprint identification services and CJIS systems control are managed within the same state agency, the repository manager and CSO may be the same person.

Root (Rooting, Rooted) — The process of attaining privileged control (known as "root access") of a device running the Android operating system that ultimately allows a user the ability to alter or replace system applications and settings, run specialized applications that require administrator-level permissions, or perform other operations that are otherwise not allowed.

Salting — The process of applying a non-secret value to data prior to applying a cryptographic process, such as hashing. This process changes the value to be hashed in a manner designed to ensure an attacker cannot reuse the results of computations for one instance.

Secondary Dissemination — The promulgation of CJI from a releasing agency to an authorized recipient agency when the recipient agency has not been previously identified in a formal information exchange agreement.

Security Addendum (SA) — A uniform addendum to an agreement between the government agency and a private contractor, approved by the Attorney General of the United States, which specifically authorizes access to criminal history record information, limits the use of the information to the purposes for which it is provided, ensures the security and confidentiality of the information consistent with existing regulations and the CJIS Security Policy, provides for sanctions, and contains such other provisions as the Attorney General may require.

Sensitive But Unclassified (SBU) — Designation of information in the United States federal government that, though unclassified, often requires strict controls over its distribution. SBU is a broad category of information that includes material covered by such designations as For Official Use Only (FOUO), Law Enforcement Sensitive (LES), Sensitive Homeland Security Information, Security Sensitive Information (SSI), Critical Infrastructure Information (CII), etc. Some categories of SBU information have authority in statute or regulation (e.g., SSI, CII) while others, including FOUO, do not. As of May 9, 2008, the more appropriate terminology to use is Controlled Unclassified Information (CUI).

Server/Client Computer Certificate (device-based) — Digital certificates that are issued to servers or client computers or devices by a CA and used to prove device identity between server and/or client computer devices during the authentication process.

Service — The organized system of apparatus, appliances, personnel, etc, that supply some tangible benefit to the consumers of this service. In the context of CJI, this usually refers to one of the applications that can be used to process CJI.

Shredder — A device used for shredding documents, often as a security measure to prevent unapproved persons from reading them. Strip-cut shredders, also known as straight-cut or spaghetti-cut, slice the paper into long, thin strips but are not considered secure. Cross-cut shredders provide more security by cutting paper vertically and horizontally into confetti-like pieces.

Smartphone — See pocket/handheld mobile devices.

Social Engineering — The act of manipulating people into performing actions or divulging confidential information. While similar to a confidence trick or simple fraud, the term typically applies to trickery or deception for the purpose of information gathering, fraud, or computer system access; in most cases the attacker never comes face-to-face with the victim.

Software Patch — A piece of software designed to fix problems with, or update, a computer program or its supporting data. This includes fixing security vulnerabilities and other bugs and improving the usability or performance. Though meant to fix problems, poorly designed patches can sometimes introduce new problems. As such, patches should be installed in a test environment prior to being installed in a live, operational system. Patches often can be found in multiple locations but should be retrieved only from sources agreed upon through organizational policy.

State and Federal Agency User Agreement — A written agreement that each CSA or SIB Chief shall execute with the FBI CJIS Division stating their willingness to demonstrate conformance with the FBI CJIS Security Policy prior to the establishment of connectivity between organizations. This agreement includes the standards and sanctions governing use of CJIS systems, as well as verbiage to allow the FBI to periodically audit the CSA as well as to allow the FBI to penetration test its own network from the CSA's interfaces to it.

State Compact Officer — The representative of a state that is party to the National Crime Prevention and Privacy Compact, and is the chief administrator of the state's criminal history record repository or a designee of the chief administrator who is a regular full-time employee of the repository.

State Identification Bureau (SIB) — The state agency with the responsibility for the state's fingerprint identification services.

State Identification Bureau (SIB) Chief — The SIB Chief is the designated manager of state's SIB. If both state fingerprint identification services and CJIS systems control are managed within the same state agency, the SIB Chief and CSO may be the same person.

State of Residency — A state of residency is the state in which an individual claims and can provide documented evidence as proof of being his/her permanent living domicile. CJIS Systems Officers have the latitude to determine what documentation constitutes acceptable proof of residency.

Sur Name — The last name or family name of the user.

Sworn Law Enforcement Officer Indicator — True if the user is a sworn law enforcement officer (SLEO), false otherwise. Usage information: An IDP may assert that a user is a SLEO if all of the following conditions are true.

1. The user is a full-time employee of a state-recognized law enforcement agency.
2. The user is authorized (has the authority) to make an arrest.
3. The user is certified by a State Certifying Authority (i.e., Peace Officer Standards and Training (POST)), or equivalent.

Alternatively, an IDP may assert that a user is a SLEO if the user is a full time employee of a state-recognized law enforcement agency, acting on behalf of a SLEO, in performance of the user's assigned duties. Legal values for this attribute are "true", "false", "1", and "0", where "1" indicates true and "0" indicates false.

Symmetric Encryption — A type of encryption where the same key is used to encrypt and decrypt a message. Symmetric encryption is also known as secret key encryption.

System — Refer to connections to the FBI's criminal justice information repositories and the equipment used to establish said connections. In the context of CJI, this usually refers to applications and all interconnecting infrastructure required to use those applications that process CJI.

Tablet Devices — Tablet devices are mobile devices with a limited-feature operating system (e.g., iOS, Android, Windows RT, etc.). Tablets typically consist of a touch screen without a permanently attached keyboard intended for transport via vehicle mount or portfolio-sized carry case but not on the body. This definition does not include pocket/handheld devices (e.g., smartphones) or mobile devices with full-featured operating systems (e.g., laptops).

Telephone Number — The telephone number for a telecommunication device by which the user may be contacted.

Terminal Agency Coordinator (TAC) — Serves as the point-of-contact at the local agency for matters relating to CJIS information access. A TAC administers CJIS systems programs within the local agency and oversees the agency's compliance with CJIS systems policies.

Unique Subject Id — A persistent unique identifier for the subject or user that identifies both the subject or user and their identity provider. The identity provider should be identified by a fully qualified domain name.

User Certificate (user-based) — Digital certificates that are unique and issued to individuals by a CA. Though not always required to do so, these specific certificates are often embedded on smart cards or other external devices as a means of distribution to specified users. This certificate is used when individuals need to prove their identity during the authentication process.

Virtual Escort — Authorized personnel who actively monitor a remote maintenance session on Criminal Justice Information (CJI)-processing systems. The escort must have the ability to end the session at any time deemed necessary to ensure the protection and integrity of CJI at all times.

Virtual Machine (VM) — See Guest Operating System

Virtualization — Refers to a methodology of dividing the resources of a computer (hardware and software) into multiple execution environments, by applying one or more concepts or technologies such as hardware and software partitioning, time-sharing, partial or complete machine simulation or emulation allowing multiple operating systems, or images, to run concurrently on the same hardware.

Voice over Internet Protocol (VoIP) — A set of software, hardware, and standards designed to make it possible to transmit voice over packet switched networks, either an internal Local Area Network, or across the Internet.

Wireless Access Point — A wireless access point is a device that logically connects a wireless client device to an organization's enterprise network which processes unencrypted CJI.

Wireless (Wi-Fi) Hotspot — A wireless (Wi-Fi) hotspot is a zone or area within a fixed location allowing wireless connectivity to the Internet typically through a wired connection. Hotspots are typically available in public areas such as airports, hotels and restaurants.

APPENDIX B: ACRONYMS

Acronym	Term
AA	Advanced Authentication
AC	Agency Coordinator
ACL	Access Control List
AES	Advanced Encryption Standard
AP	Access Point
APB	Advisory Policy Board
BD-ADDR	Bluetooth-Enabled Wireless Devices and Addresses
BYOD	Bring Your Own Device
CAD	Computer-Assisted Dispatch
CAU	CJIS Audit Unit
CFR	Code of Federal Regulations
CGA	Contracting Government Agency
CHRI	Criminal History Record Information
CISA	Cybersecurity & Infrastructure Security Agency
CJA	Criminal Justice Agency
CJI	Criminal Justice Information
CJIS	Criminal Justice Information Services
ConOps	Concept of Operations
CSA	CJIS Systems Agency
CSIRC	Computer Security Incident Response Capability
CSO	CJIS Systems Officer
CUI	Controlled Unclassified Information

DAA	Designated Approving Authority
DoJ	Department of Justice
DoJCERT	DoJ Computer Emergency Response Team
FBI	Federal Bureau of Investigation
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FOUO	For Official Use Only
HIDS	Host-based Intrusion Detection System
HIPS	Host-based Intrusion Prevention System
HTTP	Hypertext Transfer Protocol
IAFIS	Integrated Automated Fingerprint Identification System
IDS	Intrusion Detection System
III	Interstate Identification Index
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSEC	Internet Protocol Security
ISA	Interconnection Security Agreement
ISO	Information Security Officer
IT	Information Technology
LASO	Local Agency Security Officer
LEEP	Law Enforcement Enterprise Portal
LMR	Land Mobile Radio
MAC	Media Access Control

MCA	Management Control Agreement
MDM	Mobile Device Management
MITM	Man-in-the-Middle
MOU	Memorandum of Understanding
MS-ISAC	Multi-State Information Sharing & Analysis Center
NARA	National Archives and Records Administration
NCIC	National Crime Information Center
NCJA	Noncriminal Justice Agency
NICS	National Instant Criminal Background Check System
NIDS	Network-based Intrusion Detection System
NIPS	Network-based Intrusion Prevention System
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
ORI	Originating Agency Identifier
OTP	One-time Password
PBX	Private Branch Exchange
PCSC	Preventing and Combating Serious Crime
PDA	Personal Digital Assistant
PII	Personally Identifiable Information
PIN	Personal Identification Number
PKI	Public Key Infrastructure
POC	Point-of-Contact
PSTN	Public Switched Telephone Network
QA	Quality Assurance

QoS	Quality of Service
RCMP	Royal Canadian Mounted Police
RF	Radio Frequency
SA	Security Addendum
SCO	State Compact Officer
SIB	State Identification Bureau
SIG	Special Interest Group
SP	Special Publication
SPRC	Security Policy Resource Center
SSID	Service Set Identifier
TAC	Terminal Agency Coordinator
TSC	Threat Screening Center
TLS	Transport Layer Security
UCN	Universal Control Number
USCERT	U.S. Computer Emergency Readiness Team
VLAN	Virtual Local Area Network
VM	Virtual Machine
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

APPENDIX C: NETWORK TOPOLOGY DIAGRAMS

Network diagrams, i.e., topological drawings, are an essential part of solid network security. Through graphical illustration, a comprehensive network diagram provides the “big picture” – enabling network managers to quickly ascertain the interconnecting nodes of a network for a multitude of purposes, including troubleshooting and optimization. Network diagrams are integral to demonstrating the manner in which each agency ensures criminal justice data is afforded appropriate technical security protections and is protected during transit and at rest.

The following diagrams, labeled Appendix C.1-A through C.1-D, are examples for agencies to utilize during the development, maintenance, and update stages of their own network diagrams. By using these example drawings as a guideline, agencies can form the foundation for ensuring compliance with Section 5.7.1.2 of the CJIS Security Policy.

The purpose for including the following diagrams in this Policy is to aid agencies in their understanding of diagram expectations and should not be construed as a mandated method for network topologies. It should also be noted that agencies are not required to use the identical icons depicted in the example diagrams and should not construe any depiction of a particular vendor product as an endorsement of that product by the FBI CJIS Division.

Appendix C.1-A is a conceptual overview of the various types of agencies that can be involved in handling of CJI, and illustrates several ways in which these interconnections might occur. This diagram is not intended to demonstrate the level of detail required for any given agency’s documentation, but it provides the reader with some additional context through which to digest the following diagrams. Take particular note of the types of network interfaces in use between agencies, in some cases dedicated circuits with encryption mechanisms, and in other cases VPNs over the Internet. This diagram attempts to show the level of diversity possible within the law enforcement community. These diagrams in no way constitute a standard for network engineering, but rather, for the expected quality of documentation.

The next three topology diagrams, C.1-B through C.1-D, depict conceptual agencies. For C.1-B through C.1-D, the details identifying specific “moving parts” in the diagrams by manufacturer and model are omitted, but it is expected that any agencies producing such documentation will provide diagrams with full manufacturer and model detail for each element of the diagram. Note that the quantities of clients should be documented in order to assist the auditor in understanding the scale of assets and information being protected.

Appendix C.1-B depicts a conceptual state law enforcement agency’s network topology and demonstrates a number of common technologies that are in use throughout the law enforcement community (some of which are compulsory per CJIS policy, and some of which are optional) including Mobile Broadband cards, VPNs, Firewalls, Intrusion Detection Devices, VLANs, and so forth. Note that although most state agencies will likely have highly-available configurations, the example diagram shown omits these complexities and only shows the “major moving parts” for clarity but please note the Policy requires the logical location of all components be shown. The level of detail depicted should provide the reader with a pattern to model future documentation from, but should not be taken as network engineering guidance.

Appendix C.1-C depicts a conceptual county law enforcement agency. A number of common technologies are presented merely to reflect the diversity in the community, including proprietary

Packet-over-RF infrastructures and advanced authentication techniques, and to demonstrate the fact that agencies can act as proxies for other agencies.

Appendix C.1-D depicts a conceptual municipal law enforcement agency, presumably a small one that lacks any precinct-to-patrol data communications. This represents one of the smallest designs that could be assembled that, assuming all other details are properly considered, would meet the criteria for Section 5.7.1.2. This diagram helps to demonstrate the diversity in size that agencies handling criminal justice data exhibit.

Figure C-1-A Overview: Conceptual Connections Between Various Agencies

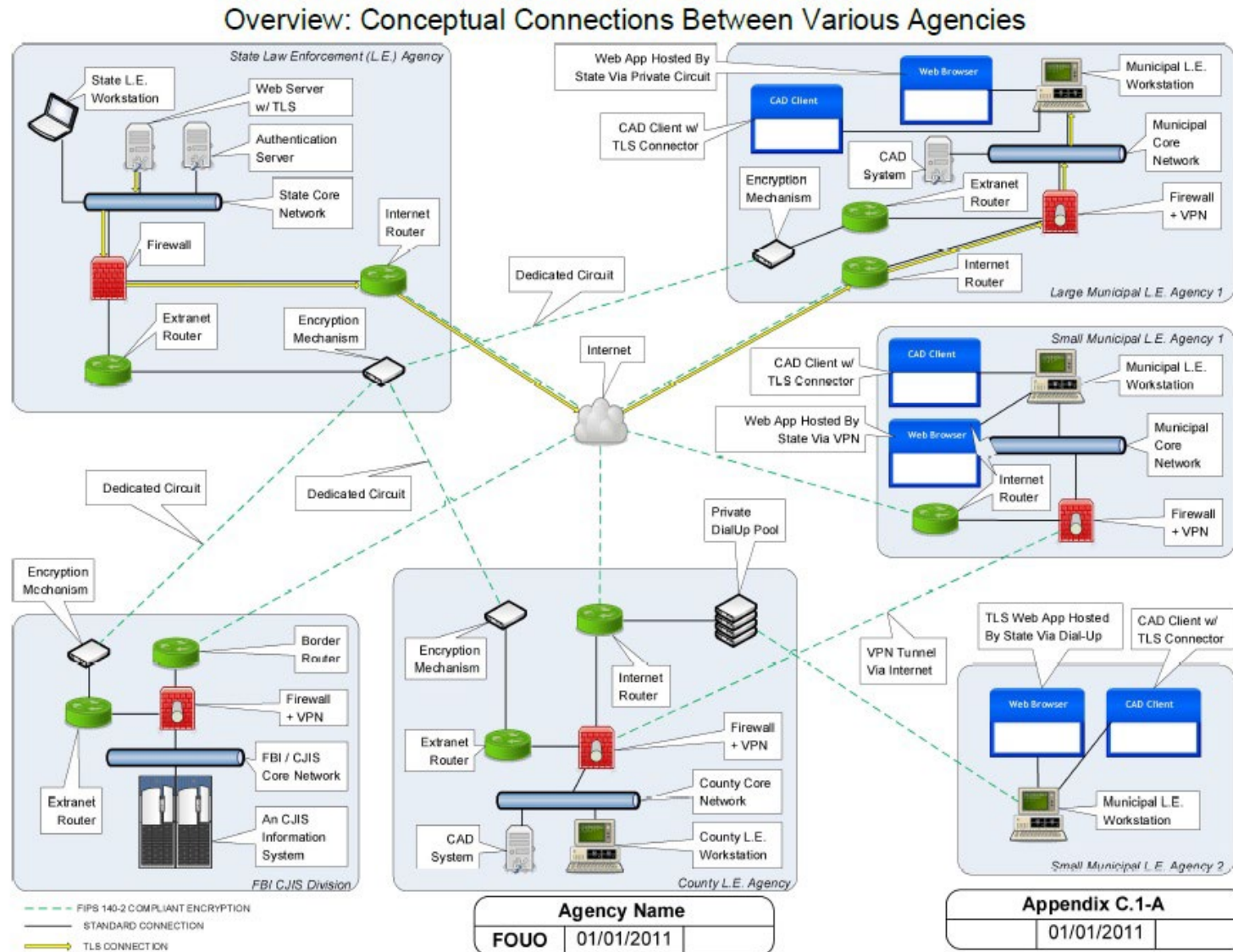


Figure C-1-B Conceptual Topology Diagram for a State Law Enforcement Agency

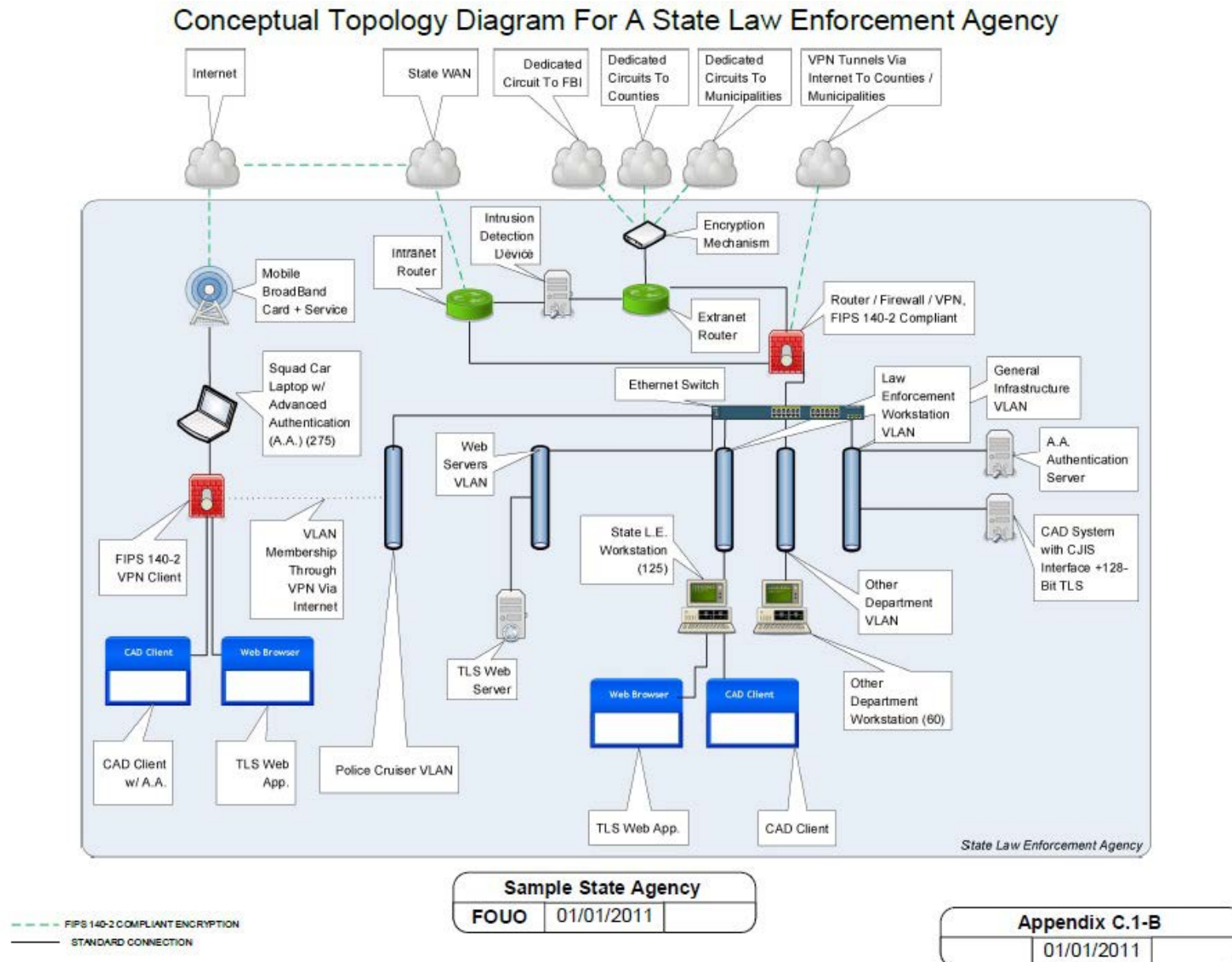


Figure C-1-C Conceptual Topology Diagram for a County Law Enforcement Agency

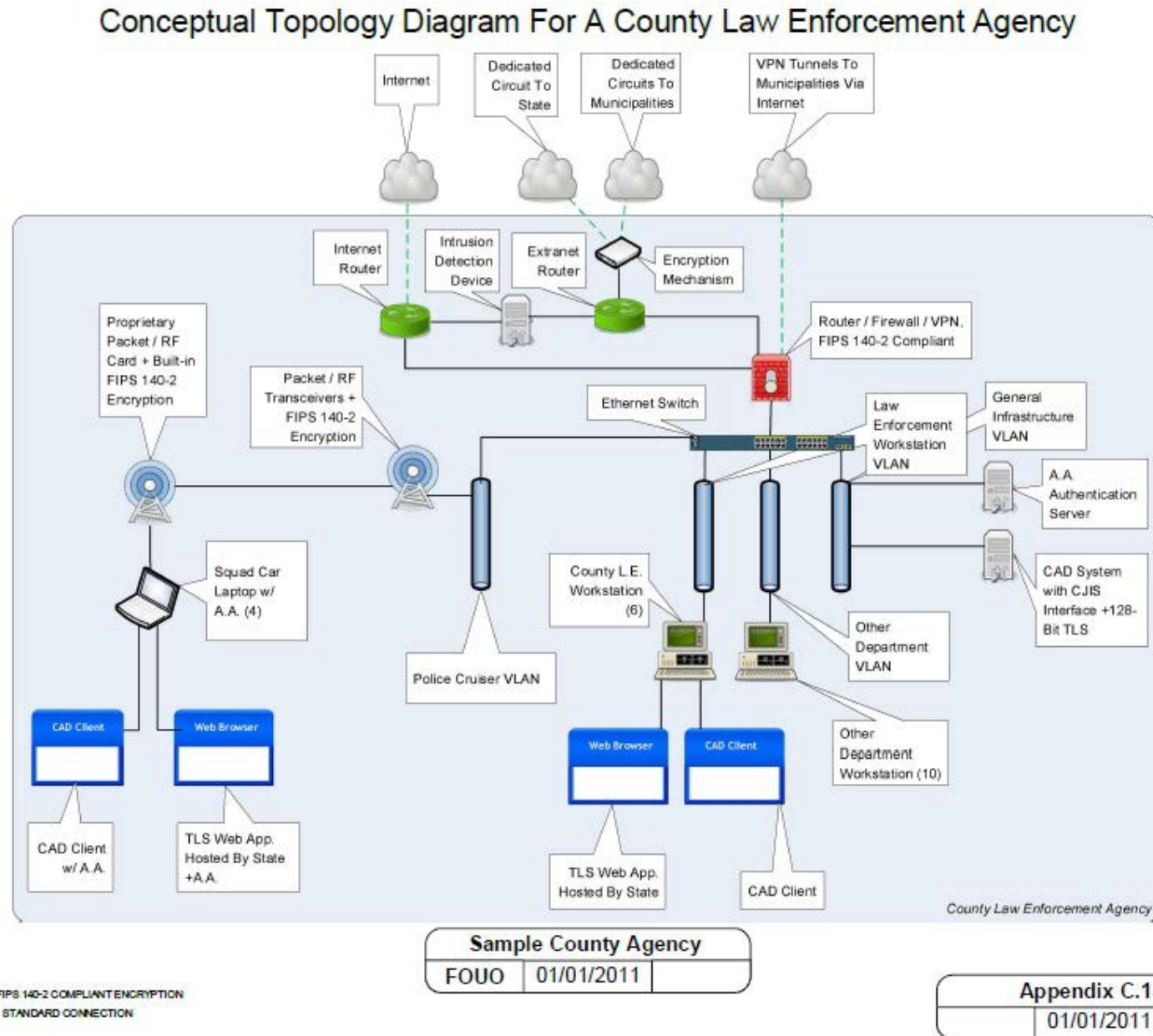
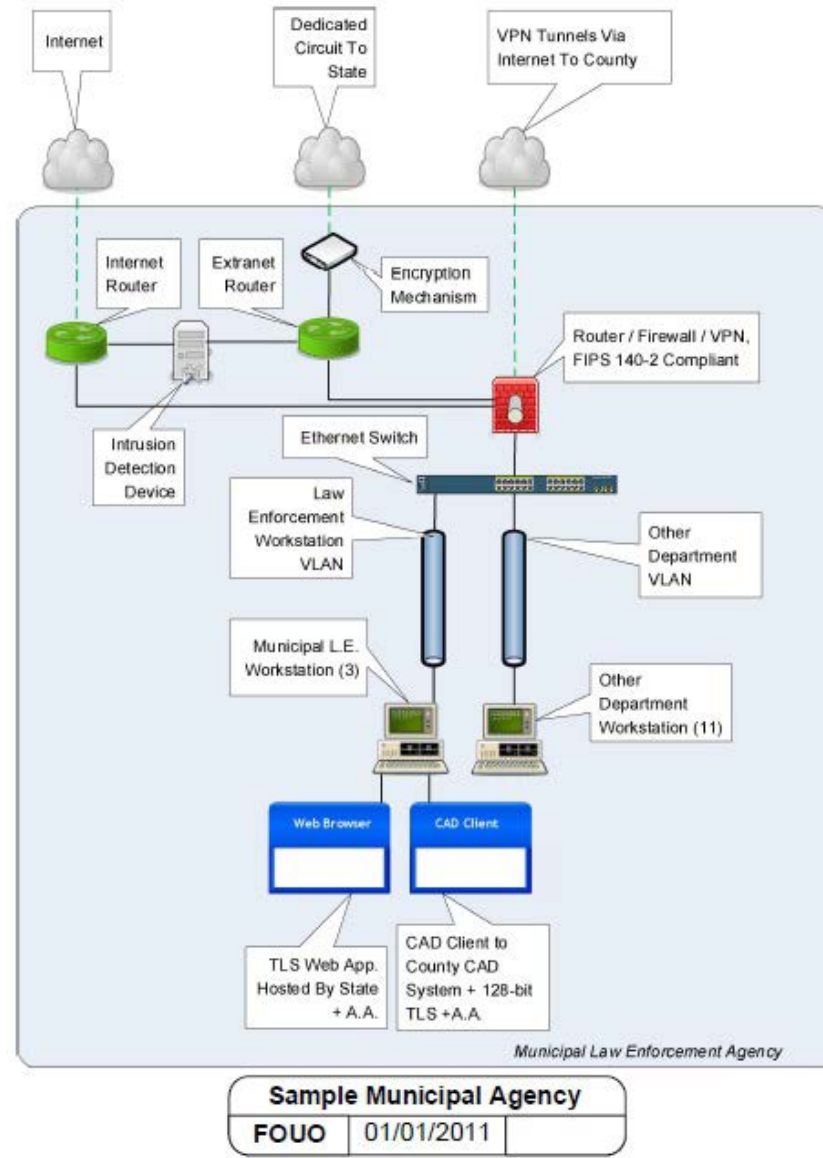


Figure C-1-D Conceptual Topology Diagram for a Municipal Law Enforcement Agency

Conceptual Topology Diagram For A Municipal Law Enforcement Agency



APPENDIX D: SAMPLE INFORMATION EXCHANGE AGREEMENTS

This appendix contains sample information exchange agreements.

D.1 CJIS User Agreement

CRIMINAL JUSTICE INFORMATION SERVICES (CJIS) DIVISION'S SYSTEM AND PROGRAM USER AGREEMENT

The FBI's CJIS Division provides state-of-the-art systems, programs, and services to the federal, state, local, tribal, regional, territorial, and foreign criminal and noncriminal justice communities. Through a shared management concept, the CJIS Division's systems, programs, and services are administered and maintained by the FBI's CJIS Division and managed in cooperation with the CJIS Advisory Policy Board (APB) and the Council established by the National Crime Prevention and Privacy Compact Act of 1998 (Compact). The CJIS Division's System and Program User Agreement (hereafter referenced as the User Agreement) covers the following: Law Enforcement Enterprise Portal (LEEP); National Crime Information Center (NCIC); National Instant Criminal Background Check System (NICS); National Data Exchange (N-DEx) System; Next Generation Identification (NGI) System; and the Uniform Crime Reporting (UCR) Program.

This User Agreement is intended to identify the categories of users, as defined by the *CJIS Security Policy (CJISSECPOL)*, and outlines the roles and responsibilities associated with participating in the CJIS Division's systems, programs, and services available to the above-listed criminal and noncriminal justice communities. This User Agreement identifies additional documentation as a valuable resource available to those individuals responsible for reviewing and signing the User Agreement.

PART 1-USER DEFINITIONS

A **CJIS Systems Agency (CSA)** is a duly authorized state, federal, international, tribal, or territorial criminal justice agency on the CJIS network providing statewide (or equivalent) service to its criminal justice users with respect to the criminal justice information (CJI) from various systems managed by the FBI's CJIS Division. There shall be only one CSA per state or territory. In federal agencies, the CSA may be the interface or switch to other federal agencies connecting to FBI CJIS Division's systems.

A **CJIS Systems Officer (CSO)** is an individual located within the CSA responsible for the administration of the CJIS network for the CSA.

An **Interface Agency (IA)** is a criminal justice agency (including law enforcement) or any federally authorized agency/entity, other than a CSA or State Identification Bureau (SIB), that leverages a direct connection to the FBI CJIS Division.

An **IA official** is an employee of the IA responsible for planning necessary hardware, software, funding, and training for the IA's authorized access to the CJIS Division's systems. The IA official shall not be a contract employee.

A **SIB** is the state (to include United States (U.S.) territories) agency with the responsibility for the state's fingerprint identification services.

An **SIB Chief** is the designated manager of the state's SIB. If both state fingerprint identification services and CJIS systems control are managed within the same state agency, the SIB Chief and CSO may be the same person.

A **state Compact officer** is the representative of a state that is party to the Compact and is the chief administrator of the state's criminal history record repository or a designee of the chief administrator who is a regular full-time employee of the repository.

The **FBI Compact officer** is appointed by the Director of the FBI and is responsible for administering the Compact within the Department of Justice and other federal agencies.

PART 2-CJIS DIVISION'S SYSTEMS, SERVICES, PROGRAMS AND RESPONSIBILITIES

The FBI's CJIS Division makes available access to the following systems and major programs (Note: Place a checkmark in the bulleted box to indicate use of specific service(s) by the agency reviewing and signing this User Agreement (applicable documents identified in Part 3)):

- ☐ LEEP
- ☐ NCIC
- ☐ NICS
- ☐ N-DEx
- ☐ NGI
- ☐ UCR

The FBI CJIS Division supports a multitude of services within the above-listed systems and programs (e.g., Interstate Identification Index (III) within NGI, NCIC offline search, UCR's Law Enforcement Suicide Data Collection, and LEEP's virtual command centers).

The FBI's CJIS Division provides the following to its authorized users, as applicable:

1. Operational, technical, and investigative assistance.
2. Secure telecommunication methods, such as wide area network (WAN) and virtual private network (VPN) connections.
3. Timely information on the CJIS Division's systems, programs, and services, by means of procedures and operating manuals, policy and implementation guides, code manuals, technical and operational updates, web pages, presentations, brochures, various newsletters, CJIS Information Letters, frequently asked questions, and other relevant documents.

4. On-site and virtual training, assistance, and system and program reference materials. The FBI's CJIS Division may prioritize on-site training opportunities to CSAs, SIBs, or IAs with open compliance findings, FBI priority initiatives, or other time-sensitive matters impacting the criminal and noncriminal justice communities.
5. Ongoing assistance through meetings and briefings to discuss operational and policy issues.
6. The CJIS Advisory Process through which authorized users have input as to the policies and procedures governing the operation of CJIS systems, programs, and services.
7. The Compact Office through education and assistance concerning the noncriminal justice use of the III of the NGI System, including facilitating engagement with the Compact Council, as needed.
8. Formal audits to ensure compliance with applicable statutes, regulations, and policies.

PART 3-CJIS DIVISION'S SYSTEMS AND PROGRAM DOCUMENTS AND AUTHORITIES

The following documents and authorities are incorporated by reference and made part of this User Agreement regarding agency access and use; this list is not all inclusive. Other policies, regulations, and manuals will be developed, published, and/or amended as CJIS Division systems, programs, and services evolve. Please contact the appropriate program office and visit the FBI CJIS Division's website for additional information: www.fbi.gov/cjis.

Security and Information Exchange Documents

CJISSECPOL

The CJISSECPOL provides criminal justice and noncriminal justice agencies with the minimum set of security requirements for access to FBI CJIS Division systems and information and to protect and safeguard CJI.

Information Exchange Package Documentation (IEPD)

An IEPD is a specification for a data exchange and defines a particular data exchange for a system.

Enterprise Documents

CJIS Information Letters

These letters provide users of CJIS Division's systems and programs with policy and procedural updates.

CSO Reference Guide

The purpose of this guide is to provide an overview of the roles and responsibilities of the CSO position.

LEEP Documents

LEEP Procedures and Operations Manual

This manual addresses the roles, responsibilities, and commitments between Identity Providers, Service Providers, and the FBI.

NCIC Documents

NCIC Operating Manual

This manual provides guidelines on the proper operation and use of the NCIC System, including the standards, procedures, formats, rules, and criteria.

NCIC Technical and Operational Updates (TOUs)

TOUs are documents that describe technical and operational changes to the NCIC System.

NICS Documents

NICS Policy Reference Guide

This manual serves as a training guide for NICS Point-of-Contact states who are processing name-based background checks through NICS before transferring a firearm to a prospective transferee.

Disposition of Firearms (DoF) User Guide

This manual serves as a training guide for law enforcement and criminal justice agencies disposing of (returning) firearms.

NICS Resource Entry and Maintaining Entries into the NICS Indices User Guide

This manual serves as a guide to sufficient source documentation to support a NICS Indices entry upon appeal or audit.

NICS Indices Reference Guide for Contributors

This manual serves as a guide for entering information into the NICS Indices.

N-DEx Documents

N-DEx Policy and Operating Manual

This manual applies to all entities with access to, or who operate in support of, N-DEx System, services, and information.

NGI Documents

III/National Fingerprint File (NFF) Operational and Technical Manual

This manual describes the III and NFF programs, including technical and operational details; procedures for entering, maintaining, and updating III and NFF records; and requirements for criminal and noncriminal fingerprint submissions.

III TOUs

TOUs are documents that describe technical and operational changes to the III System.

Electronic Biometric Transmission Specification (EBTS)

The purpose of the EBTS is to provide standards for electronically encoding and transmitting biometric images, identification, and arrest data which extends the American National Standards Institute/National Institute of Standards and Technology and Information Technology Laboratory standard. These standards ensure data is formatted for acceptance into NGI.

Compact Council's Security and Management Control Outsourcing Standards

These documents provide noncriminal justice agencies with information on the required procedures, responsibilities, and controls to maintain adequate security and integrity of criminal history record information (CHRI) while under the control or management of an outsourced, third-party contractor.

NGI Interstate Photo System (IPS) Policy and Reference Guide

This guide is made available to authorized law enforcement users and describes the policy and technical requirements for authorized use of the NGI IPS, as well as the best practices for NGI IPS users. It describes the types of NGI IPS enrollment and search transactions accepted, responses returned, training required, and additional resources available for NGI IPS users.

NGI Rap Back Service Criminal Justice Policy and Implementation Guide

This guide informs the SIBs and federal agencies of the policy and technical requirements for participation in the criminal justice Rap Back Service.

NGI Rap Back Service Noncriminal Justice Policy and Implementation Guide

This guide provides policy, technical, legal, and privacy requirements to the SIBs, federal submitting agencies, and authorized contractors who choose to participate in the FBI's NGI Noncriminal Justice Rap Back Service.

NGI Rap Back Service Noncriminal Justice Outsourcing Policy and Implementation Guide

This guide provides direction on the required policies and operations for FBI-approved channelers and nonchannelers who assist an authorized recipient with their noncriminal justice participation in the FBI's NGI Rap Back Service.

NGI Repository for Individuals of Special Concern (RISC) Policy and Implementation Guide

This guide is for the use of CSAs, vendors, and authorized criminal law enforcement agency interested in the mobile fingerprint identification search of the NGI RISC. It defines the types of search transactions that are accepted, the types of responses returned to contributors, and the system description.

NGI Iris Service Policy and Implementation Guide

This guide includes the policy and technical requirements for authorized criminal justice agency users to utilize the NGI Iris Service. It defines the types of NGI Iris Service enrollments and search transactions that are accepted, the responses returned, and references to additional technical resources.

UCR Documents

NIBRS User Manual

This manual is used to assist law enforcement agencies in reporting their crime statistics via NIBRS. This manual addresses NIBRS policies, including but not limited to, the types of offenses reported via NIBRS and guidelines for an agency to become certified to submit NIBRS data to the FBI.

NIBRS Technical Specification

This manual provides information necessary to create proper UCR NIBRS flat file submissions and is to be used in conjunction with the *NIBRS User Manual*.

Hate Crime Data Collection Guidelines and Training Manual

This manual is intended to assist law enforcement agencies in establishing an updated hate crime training program to allow their personnel to collect and submit hate crime data to the FBI's UCR Program.

Cargo Theft User Manual

This manual identifies policy and provides information regarding the types of offenses that constitute a cargo theft incident, how to identify a cargo theft, and guidelines for reporting cargo theft.

National Use-of-Force Data Collection Flat File and Bulk Load Technical Specification

This manual provides the record layout for report segments and related data elements. The bulk load feature enables report submissions outside of the web application interface.

Authorities

Title 28, United States Code (U.S.C.), Section 534

Among other things, 28 U.S.C. § 534 authorizes the United States Attorney General to collect, preserve, and exchange identification, criminal identification, crime, and other records.

Title 28, Code of Federal Regulations (C.F.R.), Part 20 and the Appendix

The purpose of these regulations is to ensure that CHRI, wherever it appears, is collected, stored, and disseminated in a manner to ensure the accuracy, completeness, currency, integrity, and security of such information and to protect individual privacy. These regulations apply to authorized federal, state, local, tribal, foreign, and international criminal justice agencies to the extent that they access the various criminal justice information systems managed by the CJIS Division or use or disseminate the records and information residing in those systems.

28 C.F.R., Part 25

The purpose of this subpart is to establish policy and procedures implementing the Brady Handgun Violence Prevention Act.

28 C.F.R. § 50.12

This section is intended to ensure that all relevant criminal record information is made available to provide for the public safety and further to protect the interest of the prospective employee/licensee who may be affected by the information or lack of information in an identification record.

Title 34, U.S.C. § 40311-40316

The Compact Act provides the legal framework for the noncriminal justice use of the III system and to facilitate complete decentralization of criminal history records. Established pursuant to the Compact, the Compact Council is to promulgate rules and procedures governing the use of the III system for noncriminal justice purposes.

PART 4- RESPONSIBILITIES OF THE CSA/IA/SIB

The purpose of a designated CSA/IA/SIB (also referenced as Signatory) is to unify responsibility for the administration and oversight of the users of the CJIS Division's systems, programs, and services, and ensure adherence to established procedures and policies within each Signatory federal, state, local, tribal, regional, territorial, and foreign agency and by each user. The CSA/IA/SIB may impose more stringent protection measures than outlined in this User Agreement. Such decisions shall be documented and kept current.

In addition, and as applicable, the CSO/IA official acknowledges state and FBI Compact officer responsibilities to ensure that Compact statutory provisions and rules, procedures, and standards established by the Compact Council are complied with in their respective area of responsibility.

Furthermore, this User Agreement applies to SIBs who have access to the CJIS Division's systems separate and apart from their state's CSA. In addition, and as applicable, the SIB Chief acknowledges the state Compact officers' responsibilities to ensure that Compact statutory provisions and rules, procedures, and standards are complied with in their respective area of responsibility.

To ensure continued access as set forth above, the Signatory agrees to adhere to all applicable policies of the CJIS Division including, but not limited to, the following:

1. As applicable, the Signatory agencies will provide fingerprints that meet submission criteria for all qualifying arrests. In addition, federal, state, local, tribal, regional, territorial, and foreign agencies will make their records available for interstate exchange for criminal justice and other authorized purposes unless restricted by federal, state, local, tribal, regional, territorial, and foreign laws, and, where applicable, continue to move toward participation in the III and, upon ratification of the Compact, the NFF. [Article I(4) of the National Crime Prevention and Privacy Compact Act (Title 34, United States Code, section 40316) defines criminal history records as (A) . . . information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, or release; and (B) does not include identification information such as fingerprint records if such information does not indicate involvement of the individual with the criminal justice system.]
2. Appropriate and reasonable quality assurance procedures, e.g., hit confirmation, audits for record timeliness, and validation for all CJIS Division systems, programs, and services in which they participate, e.g., biometrics, must be in place to ensure that only complete, accurate, and valid information is maintained in the CJIS Division's systems.
3. Biannual file synchronization of information entered into the III by participating agencies.
4. Each Signatory is responsible for the minimum-security measures as defined by the *CJISSECPOL*.
5. Each CSA/IA/SIB is responsible for completing a triennial audit of all agencies with access to the CJIS Division's systems through the system(s) of the CSA/IA/SIB. In addition, each authorized CSA/IA/SIB user is subject to a triennial audit by the CJIS Division.
6. Each CSA/IA/SIB shall be responsible for training requirements, including compliance with operator training mandates of the CJIS Division's systems, programs, and services, as outlined by the above-referenced systems and program documents.
7. Each CSA/IA/SIB shall be responsible for maintaining the integrity of their information systems in accordance with established policies to ensure only authorized terminal access; only authorized transaction submission; and proper protection, handling, and dissemination of CJI. Each CSA/IA/SIB shall be responsible for security incident reporting as required by the *CJISSECPOL*.

8. In the event that any state/local/tribal agency for which the designated CSA/IA/SIB is responsible receives a request pursuant to a freedom of information law, the civil or criminal discovery process, or other judicial, legislative, or administrative process, to disclose FBI information concerning the subject matter of this agreement, the designated CSA/IA/SIB will ensure that the state/local/tribal agency immediately notifies the FBI of any such request in order to allow the FBI sufficient time to seek to protect its equities through appropriate channels, if necessary. For purposes of this paragraph, FBI information includes, but is not limited to, e-mails or other correspondence with the FBI and the information referenced in Part 2, paragraphs 3 through 5 of this agreement. This provision survives the termination of this agreement.

PART 5-GENERAL PROVISIONS

Funding:

Unless otherwise agreed in writing, each signatory to this User Agreement (hereafter referenced as party) shall bear its own costs in relation to this User Agreement. Expenditures will be subject to budgetary processes and availability of funds pursuant to applicable laws and regulations. The parties expressly acknowledge that this User Agreement in no way implies that Congress will appropriate funds for such expenditures.

Termination and Other Topics

1. All activities of the parties under this User Agreement will be carried out in accordance with the above-described provisions.
2. This User Agreement may be amended or terminated by the mutual written consent of the parties' authorized representatives.
3. The parties acknowledge that this User Agreement does not alter applicable law governing any claim for civil liability arising out of any activity conducted pursuant to this User Agreement or otherwise relating to this User Agreement.
4. This User Agreement is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law or otherwise by any third party against the parties, the United States, or the officers, employees, agents, or other associated personnel thereof. No assignment of rights, duties, or obligations of this User Agreement shall be made by any party without the express written approval of a duly authorized representative of all other parties.
5. Each party agrees to notify the other party in the event of receipt of a civil claim arising from this User Agreement. The parties agree to cooperate fully with one another in the event of any investigation arising from alleged negligence or misconduct arising

from acts or omissions related to this User Agreement. Nothing in this paragraph prevents any party from conducting an independent administrative review of any incident giving rise to a claim.

6. Either party may terminate this User Agreement upon 30-days, written notification to the other party. Such notice will be the subject of immediate consultation by the parties to decide upon the appropriate course of action. In the event of such termination, the following rules apply:

- a. The parties will continue participation, financial or otherwise, up to the effective date of termination.
- b. Each party will pay the costs it incurs as a result of termination.
- c. All information and rights therein received under the provisions of this User Agreement, prior to the termination, will be retained by the parties subject to the provisions of this User Agreement.

PART 6-ACKNOWLEDGMENT AND CERTIFICATION

I hereby certify that I am a U.S. Citizen and acknowledge the duties and responsibilities as set out in this User Agreement. I acknowledge these duties and responsibilities have been developed and approved by the users of the CJIS Division's systems to ensure the reliability, confidentiality, completeness, and accuracy of all information contained in, or obtained by means of, the CJIS Division's systems. I further acknowledge that failure to comply with these duties and responsibilities may result in the imposition of non-monetary sanctions against the offending signatory agency. The APB or the Compact Council may approve sanctions to include the termination of CJIS services.

I hereby certify that I am familiar with all applicable documents that are made part of this User Agreement and all applicable federal and state laws and regulations relevant to the receipt and dissemination of information provided through the CJIS Division's systems, programs, and services.

Should the designated official vacate their position, the FBI designated federal officer must be notified via E-mail at AGMU@leo.gov. The name and telephone number of the acting CSO, IA official, or SIB chief and when known, the name and telephone number of the new CSO, IA official, or SIB chief must be provided, and a new User Agreement must be executed by the appropriate designated official. In addition, if the use and participation in the acknowledged systems and/or programs in Part 2 of this User Agreement change, a new User Agreement must be executed. In addition, this User Agreement will be reviewed every three years by the FBI CJIS Division.

This User Agreement is a formal expression of the purpose and intent of the parties and is effective when signed. It may be amended by the deletion or modification of any provision contained therein, or by the addition of new provisions, after written concurrence of the parties. The "Acknowledgment and Certification" is being executed by the appropriate authorized official in a representative capacity. Accordingly, this User Agreement will remain in effect after the authorized official vacates his/her position or until it is affirmatively amended or rescinded in writing. This User Agreement does not confer, grant, or authorize any rights, privileges, or obligations to any third party.

PART 7-SIGNATORY AUTHORITY

You are signing this CJIS Division's System and Program User Agreement as one of the following officials: CSO, IA Official, or SIB Chief.

CSO and CSA SIGNATORIES

CJIS Systems Officer
(Name)
(Title)
(Agency Name)
Date: _____

CONCURRENCE OF CSA HEAD:

CSA Head
Date: _____

INTERFACE AGENCY SIGNATORY

Interface Agency Official
(Name)
(Title)
(Agency Name)
Date: _____

CONCURRENCE OF INTERFACE AGENCY HEAD:

Interface Agency Head
Date: _____

STATE IDENTIFICATION BUREAU SIGNATORY

State Identification Bureau Chief
(Name)
(Title)
(Agency Name)

Date: _____

CONCURRENCE OF STATE IDENTIFICATION BUREAU AGENCY HEAD:

State Identification Bureau Agency Head

Date: _____

FBI CJIS DIVISION SIGNATORY

Name of Assistant Director
Assistant Director
FBI CJIS Division

Date: _____

Revised: 08/25/2023

D.2 Management Control Agreement

Management Control Agreement

Pursuant to the CJIS Security Policy, it is agreed that with respect to administration of that portion of computer systems and network infrastructure interfacing directly or indirectly with the state network (Network Name) for the interstate exchange of criminal history/criminal justice information, the (Criminal Justice Agency) shall have the authority, via managed control, to set, maintain, and enforce:

- (1) Priorities.
- (2) Standards for the selection, supervision, and termination of personnel access to Criminal Justice Information (CJI).
- (3) Policy governing operation of justice systems, computers, access devices, circuits, hubs, routers, firewalls, and any other components, including encryption, that comprise and support a telecommunications network and related criminal justice systems to include but not limited to criminal history record/criminal justice information, insofar as the equipment is used to process or transmit criminal justice systems information guaranteeing the priority, integrity, and availability of service needed by the criminal justice community.
- (4) Restriction of unauthorized personnel from access or use of equipment accessing the State network.
- (5) Compliance with all rules and regulations of the (Criminal Justice Agency) Policies and CJIS Security Policy in the operation of all information received.

“...management control of the criminal justice function remains solely with the Criminal Justice Agency.” Section 5.1.1.4

This agreement covers the overall supervision of all (Criminal Justice Agency) systems, applications, equipment, systems design, programming, and operational procedures associated with the development, implementation, and maintenance of any (Criminal Justice Agency) system to include NCIC Programs that may be subsequently designed and/or implemented within the (Criminal Justice Agency).

John Smith, CIO
Any State Department of Administration

Date

Joan Brown, CIO
(Criminal Justice Agency)

Date

D.3 Noncriminal Justice Agency Agreement & Memorandum of Understanding

MEMORANDUM OF UNDERSTANDING

BETWEEN

THE FEDERAL BUREAU OF INVESTIGATION

AND

(Insert Name of Requesting Organization)

FOR

THE ESTABLISHMENT AND ACCOMMODATION OF
THIRD-PARTY CONNECTIVITY TO THE
CRIMINAL JUSTICE INFORMATION SERVICES DIVISION'S WIDE AREA NETWORK

1. **PURPOSE:** This Memorandum of Understanding (MOU) between the Federal Bureau of Investigation (FBI) and **(insert requesting organization's name)**, hereinafter referred to as the "parties," memorializes each party's responsibilities with regard to establishing connectivity to records services accessible via the Wide Area Network (WAN) of the FBI's Criminal Justice Information Services (CJIS) Division.

2. **BACKGROUND:** The requesting organization, **(insert requesting organization's name)**, being approved for access to systems of records accessible via the CJIS WAN, desires connectivity to the CJIS WAN or via a secure Virtual Private Network (VPN) Connection (Internet) to the CJIS WAN. The CJIS Division has created a framework for accommodating such requests based on the type of connection.

In preparing for such non-CJIS-funded connectivity to the CJIS WAN, the parties plan to acquire, configure, and place needed communications equipment at suitable sites and to make electronic connections to the appropriate systems of records via the CJIS WAN.

To ensure that there is a clear understanding between the parties regarding their respective roles in this process, this MOU memorializes each party's responsibilities regarding the development, operation, and maintenance of third-party connectivity to the CJIS WAN. Unless otherwise contained in an associated contract, the enclosed terms apply. If there is a conflict between terms and provisions contained in both the contract and this MOU, the contract will prevail.

3. **AUTHORITY:** The FBI is entering into this MOU under the authority provided by Title 28, United States Code (U.S.C.), Section 534; 42 U.S.C. § 14616; and/or Title 28, Code of Federal Regulations, Part 906.

4. **SCOPE:**

a. The CJIS Division agrees to:

- i. Provide the requesting organization with a "CJIS WAN Third-Party Connectivity Package" that will detail connectivity requirements and options compatible with the CJIS Division's WAN architecture upon receipt of a signed nondisclosure statement.
- ii. Configure the requesting organization's connection termination equipment suite at Clarksburg, West Virginia, and prepare it for deployment or shipment under the CJIS WAN option. In the Secure VPN arrangement only, the third party will develop, configure, manage, and maintain its network connectivity to its preferred service provider.
- iii. Work with the requesting organization to install the connection termination equipment suite and verify connectivity.
- iv. Perform installation and/or routine maintenance on the requesting organization's third-party dedicated CJIS WAN connection termination equipment after coordinating with the requesting organization's designated point of contact (POC) and during a time when the CJIS Division's technical personnel are near the requesting organization's site.
- v. Perform periodic monitoring and troubleshooting of the requesting organization's CJIS WAN connection termination equipment. Software patches will be maintained on the dedicated CJIS WAN connected network equipment only. Under the Secure VPN option, no availability or data throughput rates will be guaranteed.
- vi. Provide 24 hours a day, 7 days a week uninterrupted monitoring from the CJIS Division's Network Operations Center.
- vii. Provide information regarding potential hardware end-of-life replacement cycles to the requesting organization for its budgeting purposes.
- viii. Maintain third-party dedicated CJIS WAN connection termination equipment as if in the CJIS Division's operational environment.
- ix. Update the appropriate software on the requesting organization's dedicated connection termination equipment connected to the CJIS WAN (i.e., Cisco

- Internetwork Operating System, SafeNet frame relay encryptor firmware, etc.) pursuant to the requesting organization's authorized maintenance contracts.
- x. Provide a POC and telephone number for MOU-related issues.

b. The **(insert requesting organization's name)** agrees to:

- i. Coordinate requests for third-party connectivity to the CJIS WAN or the Secure VPN with the CJIS Division's POC.
- ii. Purchase hardware and software that are compatible with the CJIS WAN.
- iii. Pay for the telecommunications infrastructure that supports its connection to the CJIS WAN or Secure VPN.
- iv. Maintain telecommunication infrastructure in support of Secure VPN connectivity.
- v. Provide any/all hardware and software replacements and upgrades as mutually agreed to by the parties.
- vi. Pay for all telecommunication requirements related to its connectivity.
- vii. Provide required information for dedicated service relating to Data Link Connection Identifiers, Circuit Identifier, Permanent Virtual Circuit Identifiers, Local Exchange Carrier Identifier, POC, location, etc., as determined by the parties.
- viii. Transport the CJIS WAN connection termination equipment suite to the CJIS Division for configuration and preparation for deployment under the dedicated service option.
- ix. Provide registered Internet Protocol information to be used by the requesting organization's system to the CJIS Division.
- x. Provide the CJIS Division with six months advance notice or stated amount of time for testing activities (i.e., disaster recovery exercises).
- xi. Provide the CJIS Division with applicable equipment maintenance contract numbers and level of service verifications needed to perform software upgrades on connection termination equipment.
- xii. Provide the CJIS Division with applicable software upgrade and patch images (or information allowing the CJIS Division to access such images).
- xiii. Transport only official, authorized traffic over the Secure VPN.
- xiv. Provide a POC and telephone number for MOU-related issues.

5. **FUNDING:** There are no reimbursable expenses associated with this level of support. Each party will fund its own activities unless otherwise agreed to in writing. This MOU is not an obligation or commitment of funds, nor a basis for transfer of funds, but rather is a basic statement of understanding between the parties hereto of the nature of the relationship for the connectivity efforts. Unless otherwise agreed to in writing, each party shall bear its own costs in relation to this MOU. Expenditures by each party will be subject to its budgetary processes and to the availability of funds and resources pursuant to applicable laws, regulations, and policies. The parties expressly acknowledge that the above language in no way implies that Congress will appropriate funds for such expenditures.

6. SETTLEMENT OF DISPUTES: Disagreements between the parties arising under or relating to this MOU will be resolved only by consultation between the parties and will not be referred to any other person or entity for settlement.

7. SECURITY: It is the intent of the parties that the actions carried out under this MOU will be conducted at the unclassified level. No classified information will be provided or generated under this MOU.

8. AMENDMENT, TERMINATION, ENTRY INTO FORCE, AND DURATION:

- a. All activities of the parties under this MOU will be carried out in accordance with the above – described provisions.
- b. This MOU may be amended or terminated by the mutual written consent of the parties' authorized representatives.
- c. Either party may terminate this MOU upon 30-days written notification to the other party. Such notice will be the subject of immediate consultation by the parties to decide upon the appropriate course of action. In the event of such termination, the following rules apply:
 - i. The parties will continue participation, financial or otherwise, up to the effective date of the termination.
 - ii. Each party will pay the costs it incurs as a result of the termination.
 - iii. All information and rights therein received under the provisions of this MOU prior to the termination will be retained by the parties, subject to the provisions of this MOU.

9. FORCE AND EFFECT: This MOU, which consists of nine numbered sections, will enter into effect upon signature of the parties and will remain in effect until terminated. The parties should review the contents of this MOU annually to determine whether there is a need for the deletion, addition, or amendment of any provision. This MOU is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law or otherwise by any third party against the parties, their parent agencies, the United States, or the officers, employees, agents, or other associated personnel thereof.

The foregoing represents the understandings reached between the parties.

FOR THE FEDERAL BUREAU OF INVESTIGATION

[Name]

Date

Assistant Director

Criminal Justice Information Services Division

FOR THE (insert requesting organization name)

Date

D.4 Interagency Connection Agreement

CRIMINAL JUSTICE INFORMATION SERVICES (CJIS)

Wide Area Network (WAN) USER AGREEMENT

BY INTERIM REMOTE LATENT USERS

The responsibility of the FBI CJIS Division is to provide state-of-the-art identification and information services to the local, state, federal, and international criminal justice communities, as well as the civil community for licensing and employment purposes. The data provided by the information systems administered and maintained by the FBI CJIS Division are routed to and managed in cooperation with the designated interface agency official. This information includes, but is not limited to, the Interstate Identification Index (III), National Crime Information Center (NCIC), Uniform Crime Reporting (UCR)/National Incident-Based Reporting System (NIBRS), and the Integrated Automated Fingerprint Identification System (IAFIS) programs.

In order to fulfill this responsibility, the FBI CJIS Division provides the following services to its users:

- Operational, technical, and investigative assistance;
- Telecommunications lines to local, state, federal and authorized interfaces;
- Legal and legislative review of matters pertaining to IAFIS, CJIS WAN and other related services;
- Timely information on all aspects of IAFIS, CJIS WAN, and other related programs by means of technical and operational updates, various newsletters, and other relative documents;
- Shared management through the CJIS Advisory Process and the Compact Council;

- Training assistance and up-to-date materials provided to each designated agency official, and;

- Audit.

The concept behind a designated interface agency official is to unify responsibility for system user discipline and ensure adherence to system procedures and policies within each interface agency. These individuals are ultimately responsible for planning necessary hardware, software, funding, training, and the administration of policy and procedures including security and integrity for complete access to CJIS related systems and CJIS WAN related data services by authorized agencies.

The following documents and procedures are incorporated by reference and made part of this agreement:

- *CJIS Security Policy*;

- *Title 28, Code of Federal Regulations, Part 20*;

- Computer Incident Response Capability (CIRC);

- Applicable federal and state laws and regulations.

To ensure continued access as set forth above, the designated interface agency agrees to adhere to all CJIS policies, including, but not limited to, the following:

1. The signatory criminal agency will provide fingerprints for all qualifying arrests either via electronic submission or fingerprint card that meet submission criteria. In addition, the agency will make their records available for interstate exchange for criminal justice and other authorized purposes.

2. The signatory civil agency with legislative authority will provide all qualifying fingerprints via electronic submission or fingerprint card that meet submission criteria.
3. Appropriate and reasonable quality assurance procedures must be in place to ensure that only complete, accurate, and valid information is maintained in the system.
4. Security – Each agency is responsible for appropriate security measures as applicable to physical security of terminals and telecommunications lines; Interim Distributed Imaging System (IDIS) equipment shall remain stand-alone devices and be used only for authorized purposes; personnel security to meet background screening requirements; technical security to protect against unauthorized use; data security, dissemination, and logging for audit purposes; and actual security of criminal history records. Additionally, each agency must establish an information security structure that provides for an Information Security Officer (ISO) or a security point of contact.
5. Audit – Each agency shall be responsible for complying with the appropriate audit requirements.
6. Training – Each agency shall be responsible for training requirements, including compliance with training mandates.
7. Integrity of the system shall be in accordance with FBI CJIS Division and interface agency policies. Computer incident reporting shall be implemented.

Until states are able to provide remote latent connectivity to their respective latent communities via a state WAN connection, the CJIS Division may provide direct connectivity to IAFIS via a dial-up connection or through the Combined DNA Index System (CODIS) and/or National Integrated Ballistics Information Network (NIBIN) connections. When a state implements a latent management system and is able to provide intrastate connectivity and subsequent forwarding to IAFIS, this agreement may be terminated. Such termination notice will be provided in writing by either the FBI or the state CJIS Systems Agency.

It is the responsibility of the local remote latent user to develop or acquire an IAFIS compatible workstation. These workstations may use the software provided by the FBI or develop their own software, provided it is IAFIS compliant.

The CJIS Division will provide the approved modem and encryptors required for each dial-up connection to IAFIS. The CJIS Communication Technologies Unit will configure and test the encryptors before they are provided to the user. Users requesting remote latent

connectivity through an existing CODIS and/or NIBIN connection must receive verification from the FBI that there are a sufficient number of Ethernet ports on the router to accommodate the request.

If at any time search limits are imposed by the CJIS Division, these individual agency connections will be counted toward the total state allotment.

ACKNOWLEDGMENT AND CERTIFICATION

As a CJIS WAN interface agency official serving in the CJIS system, I hereby acknowledge the duties and responsibilities as set out in this agreement. I acknowledge that these duties and responsibilities have been developed and approved by CJIS system users in order to ensure the reliability, confidentiality, completeness, and accuracy of all information contained in or obtained by means of the CJIS system. I further acknowledge that a failure to comply with these duties and responsibilities may subject our agency to various sanctions adopted by the CJIS Advisory Policy Board and approved by the Director of the FBI. These sanctions may include the termination of CJIS service.

As the designated CJIS WAN interface agency official serving in the CJIS system, I hereby certify that I am familiar with the contents of the *Title 28, Code of Federal Regulations, Part 20; CJIS Security Policy; Computer Incident Response Capability*; and applicable federal or state laws and regulations applied to IAFIS and CJIS WAN Programs for the dissemination of criminal history records for criminal and noncriminal justice purposes.

*

Signature

Print or Type

CJIS WAN Agency Official

Date

CONCURRENCE OF FEDERAL/REGULATORY AGENCY HEAD OR STATE CJIS SYSTEMS OFFICER (CSO):

*

Signature

Print or Type

*

Title

Date

State CSO

FBI CJIS DIVISION:

Signature – [Name]

Assistant Director _____

Title

Date

* If there is a change in the CJIS WAN interface agency official, the FBI Designated Federal Employee must be notified in writing 30 days prior to the change.

5/27/2004 UA modification reflects change in CTO title to CSO.

APPENDIX E: SECURITY FORUMS AND ORGANIZATIONAL ENTITIES

Online Security Forums / Organizational Entities
AntiOnline
Black Hat
CIO.com
CSO Online
CyberSpeak Podcast
FBI Criminal Justice Information Services Division (CJIS)
Forrester Security Forum
Forum of Incident Response and Security Teams (FIRST)
Information Security Forum (ISF)
Information Systems Audit and Control Association (ISACA)
Information Systems Security Association (ISSA)
Infosyssec
International Organization for Standardization (ISO)
International Information Systems Security Certification Consortium, Inc. (ISC)
Metasploit
Microsoft Developer Network (MSDN) Information Security
National Institute of Standards and Technology (NIST)
Open Web Application Security Project (OWASP)
SANS (SysAdmin, Audit, Network, Security) Institute
SC Magazine
Schneier.com
Security Focus
The Register
US Computer Emergency Response Team (CERT)
US DoJ Computer Crime and Intellectual Property Section (CCIPS)

APPENDIX F: SAMPLE FORMS

This appendix contains sample forms.

F.1 Security Incident Response Form

FBI CJIS DIVISION INFORMATION SECURITY OFFICER (ISO) SECURITY INCIDENT REPORTING FORM

NAME OF PERSON REPORTING THE INCIDENT: _____

DATE OF REPORT: _____ (mm/dd/yyyy)

DATE OF INCIDENT: _____ (mm/dd/yyyy)

POINT(S) OF CONTACT (Include Phone/Extension/Email): _____

LOCATION(S) OF INCIDENT: _____

INCIDENT DESCRIPTION: _____

SYSTEM(S) AFFECTED: _____

SYSTEM(S) AFFECTED (e.g., CAD, RMS, file server, etc.): _____

METHOD OF DETECTION: _____

ACTIONS TAKEN/RESOLUTION: _____

Copies To:

John C. Weatherly

(FBI CJIS Division ISO)

1000 Custer Hollow Road

Clarksburg, WV 26306-0102

(304) 625-3660

iso@fbi.gov

APPENDIX G: BEST PRACTICES

This appendix contains best practices.

G.1 Virtualization

Virtualization

This appendix documents security considerations for implementing and operating virtual environments that process, store, and/or transmit Criminal Justice Information.

The FBI CJIS ISO has fielded several inquiries from various states requesting guidance on implementing virtual environments within their data centers. With the proliferation of virtual environments across industry in general there is a realistic expectation that FBI CJIS Auditors will encounter virtual environments during the upcoming year. Criminal Justice Agencies (CJAs) and Noncriminal Justice Agencies (NCJAs) alike need to understand and appreciate the foundation of security protection measures required for virtual environments.

From Microsoft's Introduction to Windows Server 2008

<http://www.microsoft.com/windowsserver2008/en/us/hyperv.aspx>:

"Server virtualization, also known as hardware virtualization, is a hot topic in the IT world because of the potential for serious economic benefits. Server virtualization enables multiple operating systems to run on a single physical machine as virtual machines (VMs). With server virtualization, you can consolidate workloads across multiple underutilized server machines onto a smaller number of machines. Fewer physical machines can lead to reduced costs through lower hardware, energy, and management overhead, plus the creation of a more dynamic IT infrastructure."

From a trade publication, kernelthread.com

<http://www.kernelthread.com/publications/virtualization/>:

"Virtualization is a framework or methodology of dividing the resources of a computer into multiple execution environments, by applying one or more concepts or technologies such as hardware and software partitioning, time-sharing, partial or complete machine simulation, emulation, quality of service, and many others."

From an Open Source Software developer

<http://www.kallasoft.com/pc-hardware-virtualization-basics/>:

"Virtualization refers to virtualizing hardware in software, allowing multiple operating systems, or images, to run concurrently on the same hardware. There are two main types of virtualization software:

- *"Type-1 Hypervisor, which runs 'bare-metal' (on top of the hardware)*
- *"Type-2 Hypervisor which requires a separate application to run within an operating system*

"Type1 hypervisors usually offer the best in efficiency, while Type-2 hypervisors allow for greater support of hardware that can be provided by the operating system. For the developer, power user, and small business IT professionals, virtualization offers the same basic idea of collapsing multiple physical boxes into one. For

instance, a small business can run a web server and an Exchange server without the need for two boxes. Developers and power users can use the ability to contain different development environments without the need to modify their main operating system. Big businesses can also benefit from virtualization by allowing software maintenance to be run and tested on a separate image on hardware without having to take down the main production system.”

Industry leaders and niche developers are bringing more products to market every day. The following article excerpts, all posted during September 2008, on www.virtualization.com are examples of industry offerings.

“Microsoft and Novell partnered together for joint virtualization solution. Microsoft and Novell are announcing the availability of a joint virtualization solution optimized for customers running mixed-source environments. The joint offering includes SUSE Linux Enterprise Server configured and tested as an optimized guest operating system running on Windows Server 2008 Hyper-V, and is fully supported by both companies’ channel partners. The offering provides customers with the first complete, fully supported and optimized virtualization solution to span Windows and Linux environments.”

“Sun Microsystems today announced the availability of Sun xVM Server software and Sun xVM Ops Center 2.0, key components in its strategy. Sun also announced the addition of comprehensive services and support for Sun xVM Server software and xVM Ops Center 2.0 to its virtualization suite of services. Additionally, Sun launched xVMserver.org, a new open source community, where developers can download the first source code bundle for Sun xVM Server software and contribute to the direction and development of the product.”

“NetEx, specialist in high-speed data transport over TCP, today announced Virtual HyperIP bandwidth optimization solutions for VMware environments that deliver a threefold to tenfold increase in data replication performance. Virtual HyperIP is a software-based Data Transport Optimizer that operates on the VMware ESX server and boosts the performance of storage replication applications from vendors such as EMC, NetApp, Symantec, IBM, Data Domain, and FalconStor. Virtual HyperIP mitigates TCP performance issues that are common when moving data over wide-area network (WAN) connections because of bandwidth restrictions, latency due to distance and/or router hop counts, packet loss and network errors. Like the company’s award-winning appliance-based HyperIP, Virtual HyperIP eliminates these issues with an innovative software design developed specifically to accelerate traffic over an IP based network.”

From several sources, particularly:

<http://www.windowsecurity.com/articles/security-virtualization.html>

<http://csrc.nist.gov/publications/drafts/6--64rev2/draft-sp800-64-Revision2.pdf>

Virtualization provides several benefits:

- Make better use of under-utilized servers by consolidating to fewer machines saving on hardware, environmental costs, management, and administration of the server infrastructure.

- Legacy applications unable to run on newer hardware and/or operating systems can be loaded into a virtual environment – replicating the legacy environment.
- Provides for isolated portions of a server where trusted and untrusted applications can be ran simultaneously – enabling hot standbys for failover.
- Enables existing operating systems to run on shared memory multiprocessors.
- System migration, backup, and recovery are easier and more manageable.

Virtualization also introduces several vulnerabilities:

- Host Dependent.
- If the host machine has a problem then all the VMs could potentially terminate.
- Compromise of the host makes it possible to take down the client servers hosted on the primary host machine.
- If the virtual network is compromised then the client is also compromised.
- Client share and host share can be exploited on both instances. Potentially this can lead to files being copied to the share that fill up the drive.

These vulnerabilities can be mitigated by the following factors:

- Apply “least privilege” technique to reduce the attack surface area of the virtual environment and access to the physical environment.
- Configuration and patch management of the virtual machine and host, i.e., Keep operating systems and application patches up to date on both virtual machines and hosts.
- Install the minimum applications needed on host machines.
- Practice isolation from host and virtual machine.
- Install and keep updated antivirus on virtual machines and the host.
- Segregation of administrative duties for host and versions.
- Audit logging as well as exporting and storing the logs outside the virtual environment.
- Encrypting network traffic between the virtual machine and host IDS and IPS monitoring.
- Firewall each virtual machine from each other and ensure that only allowed protocols will transact.

G.2 Voice over Internet Protocol

Voice over Internet Protocol (VoIP)

Attribution:

The following information has been extracted from NIST Special Publication 800-58, Security Considerations for Voice over IP Systems.

Definitions:

Voice over Internet Protocol (VoIP) – A set of software, hardware, and standards designed to make it possible to transmit voice over packet switched networks, either an internal Local Area Network, or across the Internet.

Internet Protocol (IP) – A protocol used for communicating data across a packet-switched internetwork using the Internet Protocol Suite, also referred to as TCP/IP. IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses.

Summary:

Voice over Internet Protocol (VoIP) has been embraced by organizations globally as an addition to, or replacement for, public switched telephone network (PSTN) and private branch exchange (PBX) telephone systems. The immediate benefits are alluring since the typical cost to operate VoIP is less than traditional telephone services and VoIP can be installed in-line with an organization's existing Internet Protocol services. Unfortunately, installing a VoIP network is not a simple "plug-and-play" procedure. There are myriad security concerns, cost issues with new networking hardware requirements, and overarching quality of service (QoS) factors that have to be considered carefully.

What are some of the advantages of VoIP?

- a. Cost – a VoIP system is usually cheaper to operate than an equivalent office telephone system with a Private Branch Exchange and conventional telephone service.
- b. Integration with other services – innovative services are emerging that allow customers to combine web access with telephone features through a single PC or terminal. For example, a sales representative could discuss products with a customer using the

company's web site. In addition, the VoIP system may be integrated with video across the Internet, providing a teleconferencing facility.

What are some of the disadvantages of VoIP?

- a. Startup cost – although VoIP can be expected to save money in the long run, the initial installation can be complex and expensive. In addition, a single standard has not yet emerged for many aspects of VoIP, so an organization must plan to support more than one standard, or expect to make relatively frequent changes as the VoIP field develops.
- b. Security – the flexibility of VoIP comes at a price: added complexity in securing voice and data. Because VoIP systems are connected to the data network, and share many of the same hardware and software components, there are more ways for intruders to attack a VoIP system than a conventional voice telephone system or PBX.

VoIP Risks, Threats, and Vulnerabilities

This section details some of the potential threats and vulnerabilities in a VoIP environment, including vulnerabilities of both VoIP phones and switches. Threat discussion is included because the varieties of threats faced by an organization determine the priorities in securing its communications equipment. Not all threats are present in all organizations. A commercial firm may be concerned primarily with toll fraud, while a government agency may need to prevent disclosure of sensitive information because of privacy or national security concerns. Information security risks can be broadly categorized into the following three types: confidentiality, integrity, and availability, (which can be remembered with the mnemonic "CIA"). Additional risks relevant to switches are fraud and risk of physical damage to the switch, physical network, or telephone extensions.

Packet networks depend for their successful operation on a large number of configurable parameters: IP and MAC (physical) addresses of voice terminals, addresses of routers and firewalls, and VoIP specific software such as Call Managers and other programs used to place and route calls. Many of these network parameters are established dynamically every time a network component is restarted, or when a VoIP telephone is restarted or added to the network. Because there are so many places in a network with dynamically configurable parameters, intruders have a wide array of potentially vulnerable points to attack.

Vulnerabilities described in this section are generic and may not apply to all systems, but investigations by NIST and other organizations have found these vulnerabilities in a number of VoIP systems. In addition, this list is not exhaustive; systems may have security weaknesses that are not included in the list. For each potential vulnerability, a recommendation is included to eliminate or reduce the risk of compromise.

Confidentiality and Privacy

Confidentiality refers to the need to keep information secure and private. For home computer users, this category includes confidential memoranda, financial information, and security information such as passwords. In a telecommunications switch, eavesdropping on conversations is an obvious concern, but the confidentiality of other information on the switch must be protected to defend against toll fraud, voice and data interception, and

denial of service attacks. Network IP addresses, operating system type, telephone extension to IP address mappings, and communication protocols are all examples of information that, while not critical as individual pieces of data, can make an attacker's job easier.

With conventional telephones, eavesdropping usually requires either physical access to tap a line, or penetration of a switch. Attempting physical access increases the intruder's risk of being discovered, and conventional PBXs have fewer points of access than VoIP systems. With VoIP, opportunities for eavesdroppers increase dramatically, because of the many nodes in a packet network.

Switch Default Password Vulnerability

It is common for switches to have a default login/password set, e.g., admin/admin, or root/root. This vulnerability also allows for wiretapping conversations on the network with port mirroring or bridging. An attacker with access to the switch administrative interface can mirror all packets on one port to another, allowing the indirect and unnoticeable interception of all communications. Failing to change default passwords is one of the most common errors made by inexperienced users.

REMEDIATION: If possible, remote access to the graphical user interface should be disabled to prevent the interception of plaintext administration sessions. Some devices provide the option of a direct USB connection in addition to remote access through a web browser interface. Disabling port mirroring on the switch should also be considered.

Classical Wiretap Vulnerability

Attaching a packet capture tool or protocol analyzer to the VoIP network segment makes it easy to intercept voice traffic.

REMEDIATION: A good physical security policy for the deployment environment is a general first step to maintaining confidentiality. Disabling the hubs on IP Phones as well as developing an alarm system for notifying the administrator when an IP Phone has been disconnected will allow for the possible detection of this kind of attack.

ARP Cache Poisoning and ARP Floods

Because many systems have little authentication, an intruder may be able to log onto a computer on the VoIP network segment, and then send ARP commands corrupting ARP caches on sender(s) of desired traffic, then activate IP. An ARP flood attack on the switch could render the network vulnerable to conversation eavesdropping. Broadcasting ARP replies blind is sufficient to corrupt many ARP caches. Corrupting the ARP cache makes it possible to re-route traffic to intercept voice and data traffic.

REMEDIATION: Use authentication mechanisms wherever possible and limit physical access to the VoIP network segment.

Web Server interfaces

Both VoIP switches and voice terminals are likely to have a web server interface for remote or local administration. An attacker may be able to sniff plaintext HTTP packets to gain

confidential information. This would require access to the local network on which the server resides.

REMEDIATION: If possible, do not use an HTTP server. If it is necessary to use a web server for remote administration, use the more secure HTTPS (HTTP over SSL or TLS) protocol.

IP Phone Netmask Vulnerability

A similar effect of the ARP Cache Vulnerability can be achieved by assigning a subnet mask and router address to the phone crafted to cause most or all of the packets it transmits to be sent to an attacker's MAC address. Again, standard IP forwarding makes the intrusion all but undetectable.

REMEDIATION: A firewall filtering mechanism can reduce the probability of this attack. Remote access to IP phones is a severe risk.

Extension to IP Address Mapping Vulnerability

Discovering the IP address corresponding to any extension requires only calling that extension and getting an answer. A protocol analyzer or packet capture tool attached to the hub on the dialing instrument will see packets directly from the target instrument once the call is answered. Knowing the IP address of a particular extension is not a compromise in itself, but makes it easier to accomplish other attacks. For example, if the attacker is able to sniff packets on the local network used by the switch, it will be easy to pick out packets sent and received by a target phone. Without knowledge of the IP address of the target phone, the attacker's job may be much more difficult to accomplish and require much longer, possibly resulting in the attack being discovered.

REMEDIATION: Disabling the hub on the IP Phone will prevent this kind of attack. However, it is a rather simple task to turn the hub back on.

Integrity Issues

Integrity of information means that information remains unaltered by unauthorized users. For example, most users want to ensure that bank account numbers cannot be changed by anyone else, or that passwords are changed only by the user or an authorized security administrator. Telecommunication switches must protect the integrity of their system data and configuration. Because of the richness of feature sets available on switches, an attacker who can compromise the system configuration can accomplish nearly any other goal. For example, an ordinary extension could be re-assigned into a pool of phones that supervisors can listen in on or record conversations for quality control purposes. Damaging or deleting information about the IP network used by a VoIP switch results in an immediate denial of service.

The security system itself provides the capabilities for system abuse and misuse. That is, compromise of the security system not only allows system abuse but also allows the elimination of all traceability and the insertion of trapdoors for intruders to use on their next visit. For this reason, the security system must be carefully protected. Integrity threats include any in which system functions or data may be corrupted, either accidentally or as

a result of malicious actions. Misuse may involve legitimate users (i.e., insiders performing unauthorized operations) or intruders.

A legitimate user may perform an incorrect, or unauthorized, operations function (e.g., by mistake or out of malice) and may cause deleterious modification, destruction, deletion, or disclosure of switch software and data. This threat may be caused by several factors including the possibility that the level of access permission granted to the user is higher than what the user needs to remain functional.

Intrusion – An intruder may masquerade as a legitimate user and access an operations port of the switch. There are a number of serious intrusion threats. For example, the intruder may use the permission level of the legitimate user and perform damaging operations functions such as:

- Disclosing confidential data
- Causing service deterioration by modifying the switch software
- Crashing the switch
- Removing all traces of the intrusion (e.g., modifying the security log) so that it may not be readily detected

Insecure state – At certain times the switch may be vulnerable due to the fact that it is not in a secure state. For example:

- After a system restart, the old security features may have been reset to insecure settings, and new features may not yet be activated. (For example, all old passwords may have reverted to the default system-password, even though new passwords are not yet assigned.) The same may happen at the time of a disaster recovery.
- At the time of installation the switch may be vulnerable until the default security features have been replaced.

DHCP Server Insertion Attack

It is often possible to change the configuration of a target phone by exploiting the DHCP response race when the IP phone boots. As soon as the IP phone requests a DHCP response, a rogue DHCP server can initiate a response with data fields containing false information.

This attack allows for possible man in the middle attacks on the IP-media gateway, and IP Phones. Many methods exist with the potential to reboot the phone remotely, e.g., “social engineering”, ping flood, MAC spoofing (probably SNMP hooks, etc.).

REMEDIATION: If possible, use static IP addresses for the IP Phones. This will remove the necessity of using a DHCP server. Further, using a state based intrusion detection system can filter out DHCP server packets from IP Phone ports, allowing this traffic only from the legitimate server.

TFTP Server Insertion Attack

It is possible to change the configuration of a target phone by exploiting the TFTP response race when the IP phone is resetting. A rogue TFTP server can supply spurious information before the legitimate server is able to respond to a request. This attack allows an attacker to change the configuration of an IP Phone.

REMEDIATION: Using a state based intrusion detection system can filter out DHCP server packets from IP Phone ports, allowing such traffic only from the legitimate server. Organizations looking to deploy VoIP systems should look for IP Phone instruments that can download signed binary files.

Availability and Denial of Service

Availability refers to the notion that information and services be available for use when needed. Availability is the most obvious risk for a switch. Attacks exploiting vulnerabilities in the switch software or protocols may lead to deterioration or even denial of service or functionality of the switch. For example: if unauthorized access can be established to any branch of the communication channel (such as a CCS link or a TCP/IP link), it may be possible to flood the link with bogus messages causing severe deterioration (possibly denial) of service. A voice over IP system may have additional vulnerabilities with Internet connections. Because intrusion detection systems fail to intercept a significant percentage of Internet based attacks, attackers may be able to bring down VoIP systems by exploiting weaknesses in Internet protocols and services.

Any network may be vulnerable to denial of service attacks, simply by overloading the capacity of the system. With VoIP the problem may be especially severe, because of its sensitivity to packet loss or delay.

CPU Resource Consumption Attack without any account information.

An attacker with remote terminal access to the server may be able to force a system restart (shutdown all/restart all) by providing the maximum number of characters for the login and password buffers multiple times in succession. Additionally, IP Phones may reboot as a result of this attack.

In addition to producing a system outage, the restart may not restore uncommitted changes or, in some cases, may restore default passwords, which would introduce intrusion vulnerabilities.

REMEDIATION: The deployment of a firewall disallowing connections from unnecessary or unknown network entities is the first step to overcoming this problem. However, there is still the opportunity for an attacker to spoof his MAC and IP address, circumventing the firewall protection.

Default Password Vulnerability

It is common for switches to have a default login/password set, e.g., admin/admin, or root /root. Similarly, VoIP telephones often have default keypad sequences that can be used to unlock and modify network information.

This vulnerability would allow an attacker to control the topology of the network remotely, allowing for not only complete denial of service to the network, but also a port mirroring attack to the attacker's location, giving the ability to intercept any other conversations taking place over the same switch. Further, the switch may have a web server interface, providing an attacker with the ability to disrupt the network without advance knowledge of switch operations and commands. In most systems, telephones download their configuration data on startup using TFTP or similar protocols. The configuration specifies the IP addresses for Call Manager nodes, so an attacker could substitute another IP address pointing to a call manager that would allow eavesdropping or traffic analysis.

REMEDIATION: Changing the default password is crucial. Moreover, the graphical user interface should be disabled to prevent the interception of plaintext administration sessions.

Exploitable software flaws

Like other types of software, VoIP systems have been found to have vulnerabilities due to buffer overflows and improper packet header handling. These flaws typically occur because the software is not validating critical information properly. For example, a short integer may be used as a table index without checking whether the parameter passed to the function exceeds 32,767, resulting in invalid memory accesses or crashing of the system.

Exploitable software flaws typically result in two types of vulnerabilities: denial of service or revelation of critical system parameters. Denial of service can often be implemented remotely, by passing packets with specially constructed headers that cause the software to fail. In some cases the system can be crashed, producing a memory dump in which an intruder can find IP addresses of critical system nodes, passwords, or other security-relevant information. In addition, buffer overflows that allow the introduction of malicious code have been found in VoIP software, as in other applications.

REMEDIATION: These problems require action from the software vendor, and distribution of patches to administrators. Intruders monitor announcements of vulnerabilities, knowing that many organizations require days or weeks to update their software. Regular checking for software updates and patches is essential to reducing these vulnerabilities. Automated patch handling can assist in reducing the window of opportunity for intruders to exploit known software vulnerabilities.

Account Lockout Vulnerability

An attacker will be able to provide several incorrect login attempts at the telnet prompt until the account becomes locked out. (This problem is common to most password-protected systems, because it prevents attackers from repeating login attempts until the correct password is found by trying all possible combinations.)

The account is unable to connect to the machine for the set lockout time.

REMEDIATION: If remote access is not available, this problem can be solved with physical access control.

NIST Recommendations.

Because of the integration of voice and data in a single network, establishing a secure VoIP and data network is a complex process that requires greater effort than that required for data-only networks. In particular, start with these general guidelines, recognizing that practical considerations, such as cost or legal requirements, may require adjustments for the organization:

9. Develop appropriate network architecture.

- Separate voice and data on logically different networks if feasible. Different subnets with separate RFC 1918 address blocks should be used for voice and data traffic, with separate DHCP servers for each, to ease the incorporation of intrusion detection and VoIP firewall protection at the voice gateway, which interfaces with the PSTN, disallow H.323, SIP, or other VoIP protocols from the data network. Use strong authentication and access control on the voice gateway system, as with any other critical network component. Strong authentication of clients towards a gateway often presents difficulties, particularly in key management. Here, access control mechanisms and policy enforcement may help.
- A mechanism to allow VoIP traffic through firewalls is required. There are a variety of protocol dependent and independent solutions, including application level gateways (ALGs) for VoIP protocols, Session Border Controllers, or other standards-based solutions when they mature.
- Stateful packet filters can track the state of connections, denying packets that are not part of a properly originated call. (This may not be practical when multimedia protocol inherent security or lower layer security is applied, e.g., H.235 Annex D for integrity provision or TLS to protect SIP signaling).
- Use Isec or Secure Shell (SSH) for all remote management and auditing access. If practical, avoid using remote management at all and do IP PBX access from a physically secure system.
- If performance is a problem, use encryption at the router or other gateway, not the individual endpoints, to provide for Isec tunneling. Since some VoIP endpoints are not computationally powerful enough to perform encryption, placing this burden at a central point ensures all VoIP traffic emanating from the enterprise network has been encrypted. Newer IP phones are able to provide Advanced Encryption System (AES) encryption at reasonable cost. Note that Federal

Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, is applicable to all Federal agencies that use cryptographic-based security systems to protect sensitive information in computer and telecommunication systems (including voice systems) as defined in Section 5131 of the Information Technology Management Reform Act of 1996, Public Law 104-106.

10. Ensure that the organization has examined and can acceptably manage and mitigate the risks to their information, system operations, and continuity of essential operations when deploying VoIP systems.

VoIP can provide more flexible service at lower cost, but there are significant tradeoffs that must be considered. VoIP systems can be expected to be more vulnerable than conventional telephone systems, in part because they are tied in to the data network, resulting in additional security weaknesses and avenues of attack (see VoIP Risks, Threats, and Vulnerabilities section for more detailed discussion of vulnerabilities of VoIP and their relation to data network vulnerabilities).

Confidentiality and privacy may be at greater risk in VoIP systems unless strong controls are implemented and maintained. An additional concern is the relative instability of VoIP technology compared with established telephony systems. Today, VoIP systems are still maturing and dominant standards have not emerged. This instability is compounded by VoIP's reliance on packet networks as a transport medium. The public switched telephone network is ultra-reliable. Internet service is generally much less reliable, and VoIP cannot function without Internet connections, except in the case of large corporate or other users who may operate a private network. Essential telephone services, unless carefully planned, deployed, and maintained, will be at greater risk if based on VoIP.

11. Special consideration should be given to E-911 emergency services communications, because E-911 automatic location service is not available with VoIP in some cases.

Unlike traditional telephone connections, which are tied to a physical location, VoIP's packet switched technology allows a particular number to be anywhere. This is convenient for users, because calls can be automatically forwarded to their locations. But the tradeoff is that this flexibility severely complicates the provision of E-911 service, which normally provides the caller's location to the 911 dispatch office. Although most VoIP vendors have workable solutions for E-911 service, government regulators and vendors are still working out standards and procedures for 911 services in a VoIP environment. Agencies must carefully evaluate E-911 issues in planning for VoIP deployment.

12. Agencies should be aware that physical controls are especially important in a VoIP environment and deploy them accordingly.

Unless the VoIP network is encrypted, anyone with physical access to the office LAN could potentially connect network monitoring tools and tap into telephone conversations. Although conventional telephone lines can also be monitored when physical access is obtained, in most offices there are many more points to connect with a LAN without arousing suspicion. Even if encryption is used, physical access to VoIP servers and gateways may allow an attacker to do traffic analysis (i.e., determine which parties are

communicating). Agencies therefore should ensure that adequate physical security is in place to restrict access to VoIP network components. Physical security measures, including barriers, locks, access control systems, and guards, are the first line of defense. Agencies must make sure that the proper physical countermeasures are in place to mitigate some of the biggest risks such as insertion of sniffers or other network monitoring devices. Otherwise, practically speaking this means that installation of a sniffer could result in not just data but all voice communications being intercepted.

13. VoIP-ready firewalls and other appropriate protection mechanisms should be employed.

Agencies must enable, use, and routinely test the security features that are included in VoIP systems.

Because of the inherent vulnerabilities (e.g., susceptibility to packet sniffing) when operating telephony across a packet network, VoIP systems incorporate an array of security features and protocols. Organization security policy should ensure that these features are used. In particular, firewalls designed for VoIP protocols are an essential component of a secure VoIP system.

14. If practical, “softphone” systems, which implement VoIP using an ordinary PC with a headset and special software, should not be used where security or privacy are a concern.

Worms, viruses, and other malicious software are extraordinarily common on PCs connected to the internet, and very difficult to defend against. Well-known vulnerabilities in web browsers make it possible for attackers to download malicious software without a user’s knowledge, even if the user does nothing more than visit a compromised web site. Malicious software attached to email messages can also be installed without the user’s knowledge, in some cases even if the user does not open the attachment. These vulnerabilities result in unacceptably high risks in the use of “softphones”, for most applications. In addition, because PCs are necessarily on the data network, using a softphone system conflicts with the need to separate voice and data networks to the greatest extent practical.

15. If mobile units are to be integrated with the VoIP system, use products implementing Wi-Fi Protected Access (WPA), rather than 802.11 Wired Equivalent Privacy (WEP).

The security features of 802.11 WEP provide little or no protection because WEP can be cracked with publicly available software. The more recent Wi-Fi Protected Access (WPA), a snapshot of the ongoing 802.11i standard, offers significant improvements in security, and can aid the integration of wireless technology with VoIP. NIST strongly recommends that the WPA (or WEP if WPA is unavailable) security features be used as part of an overall defense-in-depth strategy. Despite their weaknesses, the 802.11 security mechanisms can provide a degree of protection against unauthorized disclosure, unauthorized network access, or other active probing attacks. However, the Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, is mandatory and binding for Federal agencies that have determined that certain information must be protected via cryptographic means. As currently defined, neither WEP nor WPA meets the FIPS 140-2 standard. In these cases, it will be necessary to employ higher level cryptographic protocols and applications such as secure shell (SSH), Transport Level Security (TLS) or Internet Protocol Security (Ipsec) with FIPS 140-2 validated

cryptographic modules and associated algorithms to protect information, regardless of whether the nonvalidated data link security protocols are used.

16. Carefully review statutory requirements regarding privacy and record retention with competent legal advisors.

Although legal issues regarding VoIP are beyond the scope of this document, readers should be aware that laws and rulings governing interception or monitoring of VoIP lines, and retention of call records, may be different from those for conventional telephone systems. Agencies should review these issues with their legal advisors. See Section 2.5 for more on these issues.

G.3 Cloud Computing

Cloud Computing

Purpose:

This paper is provided to define and describe cloud computing, discuss CJIS Security Policy (CSP) compliance, detail security and privacy, and provide general recommendations.

Attribution:

- NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing (Dec. 2011)
- NIST SP 800-145, the NIST Definition of Cloud Computing (Sept. 2011)
- NIST SP 800-146, Cloud Computing Synopsis and Recommendations (May 2011)
- CJIS Security Policy, Version 5.0

Definitions and Terms:

Cloud computing – A distributed computing model that permits on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services), software, and information.

Cloud subscriber – A person or organization that is a customer of a cloud

Cloud client – A machine or software application that accesses a cloud over a network connection, perhaps on behalf of a subscriber

Cloud provider – An organization that provides cloud services

Summary:

With many law enforcement agencies looking for ways to attain greater efficiency while grappling with reduced budgets, the idea of cloud computing to maintain data and applications is a viable business solution. But the unique security and legal characteristics of law enforcement agencies means any migration to cloud services may be challenging. Anytime the security of information and transactions must be maintained, as it must be with access to the FBI's CJIS systems and the protection of Criminal Justice Information (CJI), security and policy compliance concerns are bound to arise.

Cloud computing has become a popular and sometimes contentious topic of discussion for both the private and public sectors. This is in part because of the difficulty in describing cloud computing in general terms, because it is not a single kind of system. The “cloud” spans a spectrum of underlying technologies, configuration possibilities, service and deployment models. Cloud computing offers the ability to conveniently rent access to fully featured applications, software development and deployment environments, and computing infrastructure assets - such as network-accessible data storage and processing from a cloud service provider.

One of the benefits of cloud computing is the ability to outsource many of the technical functions agencies may not want to perform for various reasons. Ultimately, the move to cloud computing is a business and security risk decision in which the following relevant factors are given proper consideration:

- readiness of existing applications for cloud deployment
- transition costs
- life-cycle costs
- maturity of service orientation in existing infrastructure
- security and privacy requirements – federal, state, and local

Achieving CJIS Security Policy Compliance:

The question that is often asked is, “Can an Agency be compliant with the CJIS Security Policy and also cloud compute?”

Because the CJIS Security Policy is device and architecture independent (per CSP Section 2.2), the answer is yes, and this can be accomplished— assuming the vendor of the cloud technology is able to meet the existing requirements of the CJIS Security Policy.

There are security challenges that must be addressed if CJI is to be sent into or through, stored within, or accessed from the cloud.

Admittedly, the existing CJIS Security Policy requirements may be difficult for some cloud-computing vendors due to the sheer numbers and the geographic disbursement of their personnel; however, the requirements aren’t new to vendors serving the criminal justice community and many vendors have been successfully meeting the Policy requirements for years. Even so, they are the minimum security requirements which will provide an acceptable level of assurance that law enforcement and personally identifiable information (PII) will be protected when shared with other law enforcement agencies across the nation.

General CJIS Security Policy Applicability Questions

Before tackling these challenges, the cloud subscriber should first be aware of what security and legal requirements they are subject to prior to entering into any agreement with a cloud provider. Asking the following general questions will help frame the process of determining compliance with the existing requirements of the CJIS Security Policy.

- Will access to Criminal Justice Information (CJI) within a cloud environment fall within the category of remote access? (5.5.6 Remote Access)
- Will advanced authentication (AA) be required for access to CJI within a cloud environment? (5.6.2.2 Advanced Authentication, 5.6.2.2.1 Advanced Authentication Policy and Rationale)
- Does/do any cloud service provider's datacenter(s) used in the transmission or storage of CJI meet all the requirements of a physically secure location? (5.9.1 Physically Secure Location)
- Are the encryption requirements being met? (5.10.1.2 Encryption)
 - Who will be providing the encryption as required in the CJIS Security Policy (client or cloud service provider)? *Note: individuals with access to the keys can decrypt the stored files and therefore have access to unencrypted CJI.*
 - Is the data encrypted while at rest and in transit?
- What are the cloud service provider's incident response procedures? (5.3 Policy Area 3: Incident Response)
 - Will the cloud subscriber be notified of any incident?
 - If CJI is compromised, what are the notification and response procedures?
- Is the cloud service provider a private contractor/vendor?
 - If so, they are subject to the same screening and agreement requirements as any other private contractors hired to handle CJI? (5.1.1.5 Private Contractor User Agreements and CJIS Security Addendum; 5.12.1.2 Personnel Screening for Contractors and Vendors)
- Will the cloud service provider allow the CSA and FBI to conduct compliance and security audits? *Note: Cloud facilities such as datacenters in which CJI will be stored or processed should be audited as would any other datacenter housing and processing CJI.* (5.11.1 Audits by the FBI CJIS Division; 5.11.2 Audits by the CSA)

- How will event and content logging be handled? (5.4 Policy Area 4, Auditing and Accountability)
 - Will the cloud service provider handle the events and content logging required by the CJIS Security Policy and provide that upon request?
 - What are the cloud service provider's responsibilities with regard to media protection and destruction? (5.8 Policy Area 8: Media Protection)

Ultimately, the goal is to remain committed to using technology in its information sharing processes, but not at the sacrifice of the security of the information with which it has been entrusted. As stated in the CJIS Security Policy, device and architecture independence permits the use of cloud computing, but the security requirements do not change.

Cloud Utilization Scenarios

1. Encrypted CJI in a Cloud Environment–Key Management Control, Security Awareness Training, and Personnel Controls

Prior to permitting CJI to be stored or traverse through a cloud environment, the agency should ensure proper encryption key management control procedures are implemented to determine who has access and control over the encryption keys. Proper key management control is vital to CJI security as those individuals (agency or cloud employees) with access to the keys can decrypt the stored files, and therefore, have unescorted access to unencrypted CJI. This means all those individuals must be subjected to security awareness training (CJIS Security Policy section 5.2) and must meet personnel security (CJIS Security Policy Section 5.12) requirements as individuals with unescorted access to unencrypted CJI.

Note: As a best security practice, the CJIS ISO Program does not recommend allowing the cloud service provider access to the encryption keys used to protect CJI. However, it may not always be reasonable to expect the agency, criminal justice or noncriminal justice, to accomplish this task.

Note: When selecting a cloud service provider, the CJIS ISO Program reminds agencies the CJIS Security Policy sets the minimum requirements for the protection of CJI. Additional security assurances from other authorizations such as FedRAMP, StateRAMP, SOC Type 2, etc., may be leveraged, however, they do not guarantee compliance with the CJIS Security Policy.

- a. Scenario 1–Agency Stores CJI in a Cloud:

A CJA stores encrypted CJI (Backup files and drives) in a cloud service provider's environment. To access CJI, the agency will extract the CJI from the cloud to its local machine, and then decrypt the CJI. The CJI is processed, re-encrypted, and then re-uploaded to the cloud environment for storage. In this scenario, the agency always encrypts the CJI prior to placing it in the cloud and only authorized users of the agency have access to the encryption keys. Since the agency maintains the encryption

keys, the cloud service provider employees would not need to undergo fingerprint-based background checks, nor have security awareness training. These requirements are negated, because only authorized personnel with access to the keys have the ability to view this CJI in an unencrypted form.

b. Scenario 2–Agency Accesses CJI While in a Cloud:

A CJA stores CJI (files and drives) in a cloud service provider’s environment, but as part of daily operations authorized users will remotely access the encrypted CJI in the cloud. The user will decrypt the CJI while it is in the cloud’s virtual environment, process the data, and then re-encrypt the data prior to ending the remote session. The agency maintains the keys and the cloud service provider does not have access to the encryption keys. However, since the CJI is decrypted within the cloud’s virtual environment, any administrative personnel employed by the cloud provider having the ability to access the virtual environment must be identified and subjected to security awareness training and personnel security controls as described in the CJIS Security Policy.

c. Scenario 3–CJI Impact from a Cloud Datacenter Critical Systems Crash–Core Dump* Recovery:

A CJA utilizes a cloud service provider (IaaS or PaaS) to store CJI and remotely accesses the environment to process CJI. During normal operation, the cloud provider experiences systems outages within the datacenter in which CJI is processed and stored. The cloud provider’s administrators need to repair the systems and restore service using data from a core dump to return to normal operations. The cloud service provider as part of the Service Level Agreement (SLA) with the CJA has been authorized to maintain the encryption keys in order respond to such an event. The cloud administrators with such access have underwent fingerprint-based background checks and security awareness training. This allows the cloud administrators to decrypt CJI so that it is written to the core dump files for restoration following the system outage. CJI, however, is encrypted at all times except when part of the core dump files. As part of the SLA, the cloud service provider has agreed to treat the core dump files as CJI to ensure all protection are in place in compliance with the CJIS Security Policy.

Note: Writing encrypted data to a core dump corrupts the data and makes it unusable because the key no longer decrypts the data. This is problematic when attempting to recover encrypted data written to a core dump. The CJA could have ensured the cloud provider exclude encrypted data (CJI) from the core dump, but chose against it.

* Core Dump - A file of a computer’s documented memory of when a program or computer crashed. The file consists of the recorded status of the working memory at an explicit time, usually close to when the system crashed or when the program ended atypically as it presents the risk that the system failure would ensure the loss of the encrypted data.

The Cloud Model Explained:

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

The cloud model as defined by NIST consists of five essential characteristics, offers the option of three service models, and may be deployed via any of four deployment models as shown in Figure 1 below:

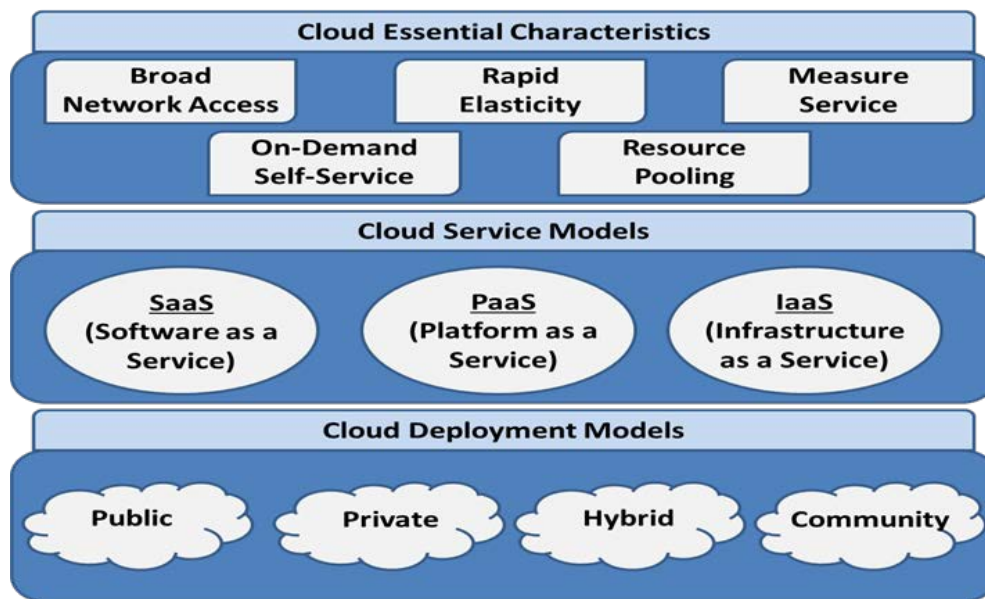


Figure 1 - Visual Depiction of the NIST Cloud Computing Definition

Essential Characteristics:

On-demand self-service

A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad network access

Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling

The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in which the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

Rapid elasticity

Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Measured service

Cloud systems automatically control and optimize resource use by leveraging a metering capability* at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

** Typically this is done on a pay-per-use or charge-per-use basis.*

Deployment Models:

Private cloud

The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Community cloud

The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public cloud

The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Hybrid cloud

The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Service Models:

Cloud providers offer different levels of service, i.e.; Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). The way CJI is placed and accessed in the cloud determines if the personnel security requirements in Section 5.12 apply. Access to encryption keys and management of the resources vary depending on what type of service is used. The SaaS offering is the most likely service wherein the cloud service provider may have access to unencrypted CJI due to software updates, patches, and management. However, through management and control of encryption keys, all service offerings may be implemented in an agency-controlled manner where the cloud service provider has no ability to access unencrypted CJI.

For cloud computing services that involve the storage, processing, or transmission of CJI, Section 5.12 security terms and requirements apply to all personnel when their unescorted logical or physical access to any information system results in the ability, right, or privilege to view, modify, or make use of unencrypted CJI. It is critical for the agency to understand the level of service and access required for each cloud implementation.

Software as a Service (SaaS)

This model provides the consumer the capability to use the provider's applications running on a cloud infrastructure*.

** A cloud infrastructure is the collection of hardware and software that enables the five essential characteristics of cloud computing. The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the cloud services being provided, and typically includes server, storage and network components. The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics. Conceptually the abstraction layer sits above the physical layer.*

The SaaS service model is often referred to as “Software deployed as a hosted service and accessed over the Internet.”

The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface.

When using the SaaS service model it should be understood that the consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Platform as a Service (PaaS)

This model provides the consumer the capability to deploy consumer-created or acquired applications* created using programming languages, libraries, services, and tools supported by the provider onto the cloud infrastructure.

** This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources.*

When using the PaaS service model the consumer may have control over the deployed applications and possibly configuration settings for the application-hosting environment, but does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage.

Infrastructure as a Service (IaaS)

This model provides the consumer the capability to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, including operating systems and applications.

When using the IaaS service model the consumer may have control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls), but does not manage or control the underlying cloud infrastructure.

Key Security and Privacy Issues:

Although the emergence of cloud computing is a recent development, insights into critical aspects of security can be gleaned from reported experiences of early adopters and also from researchers analyzing and experimenting with available cloud provider platforms and associated technologies. The sections below highlight privacy and security-related issues that are believed to have long-term significance for public cloud computing and, in many cases, for other cloud computing service models.

Because cloud computing has grown out of an amalgamation of technologies, including service oriented architecture, virtualization, Web 2.0, and utility computing, many of the privacy and security issues involved can be viewed as known problems cast in a new setting. The importance of their combined effect in this setting, however, should not be discounted. Public cloud computing does represent a thought-provoking paradigm shift from conventional norms to an open organizational infrastructure—at the extreme, *displacing applications from one organization's infrastructure to the infrastructure of another organization, where the applications of potential adversaries may also operate.*

Governance

Governance implies control and oversight by the organization over policies, procedures, and standards for application development and information technology service acquisition, as well as the design, implementation, testing, use, and monitoring of deployed or engaged services. With the wide availability of cloud computing services, lack of organizational controls over employees engaging such services arbitrarily can be a source of problems. While cloud computing simplifies platform acquisition, it doesn't alleviate the need for governance; instead, it has the opposite effect, amplifying that need.

Dealing with cloud services requires attention to the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met. Ensuring systems are secure and risk is managed is challenging in any environment and even more daunting with cloud computing. Audit mechanisms and tools should be in place to determine how data is stored, protected, and used, to validate services, and to verify policy enforcement. A risk management program should also be in place that is flexible enough to deal with the continuously evolving and shifting risk landscape.

Compliance

Compliance refers to an organization's responsibility to operate in agreement with established laws, regulations, standards, and specifications. Various types of security and privacy laws and regulations exist within different countries at the national, state, and local levels, making compliance a potentially complicated issue for cloud computing.

Law and Regulations

Cloud providers are becoming more sensitive to legal and regulatory concerns, and may be willing to commit to store and process data in specific jurisdictions and apply required safeguards for security and privacy. However, the degree to which they will accept liability in their service agreements, for exposure of content under their control, remains to be seen. Even so, organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf.

Data Location

One of the most common compliance issues facing an organization is data location. A characteristic of many cloud computing services is that data is stored redundantly in multiple physical locations and detailed information about the location of an organization's data is unavailable or not disclosed to the service consumer. This situation makes it difficult to ascertain whether sufficient safeguards are in place and whether legal and regulatory

compliance requirements are being met. External audits and security certifications can alleviate this issue to some extent, but they are not a panacea.

When information crosses borders, the governing legal, privacy, and regulatory regimes can be ambiguous and raise a variety of concerns. Consequently, constraints on the trans-border flow of sensitive data, as well as the requirements on the protection afforded the data, have become the subject of national and regional privacy and security laws and regulations.

Electronic Discovery

The capabilities and processes of a cloud provider, such as the form in which data is maintained and the electronic discovery-related tools available, affect the ability of the organization to meet its obligations in a cost effective, timely, and compliant manner. A cloud provider's archival capabilities may not preserve the original metadata as expected, causing spoliation (i.e., the intentional, reckless, or negligent destruction, loss, material alteration, or obstruction of evidence that is relevant to litigation), which could negatively impact litigation.

Trust

Under the cloud computing paradigm, an organization relinquishes direct control over many aspects of security and privacy, and in doing so, confers a high level of trust onto the cloud provider. At the same time, federal agencies have a responsibility to protect information and information systems commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction, regardless of whether the information is collected or maintained by or on behalf of the agency; or whether the information systems are used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency

Insider Access

Data processed or stored outside the physical confines of an organization, its firewall, and other security controls bring with it an inherent level of risk. The insider security threat is a well-known issue for most organizations. Incidents may involve various types of fraud, sabotage of information resources, and theft of sensitive information.

Data Ownership

The organization's ownership rights over the data must be firmly established in the service contract to enable a basis for trust and privacy of data. The continuing controversy over

privacy and data ownership rights for social networking users illustrates the impact that ambiguous terms can have on the parties involved.

Ideally, the contract should state clearly that the organization retains exclusive ownership over all its data; that the cloud provider acquires no rights or licenses through the agreement, including intellectual property rights or licenses, to use the organization's data for its own purposes; and that the cloud provider does not acquire and may not claim any interest in the data due to security. For these provisions to work as intended, the terms of data ownership must not be subject to unilateral amendment by the cloud provider.

Visibility

Continuous monitoring of information security requires maintaining ongoing awareness of security controls, vulnerabilities, and threats to support risk management decisions. Transition to public cloud services entails a transfer of responsibility to the cloud provider for securing portions of the system on which the organization's data and applications operate.

Ancillary Data

While the focus of attention in cloud computing is mainly on protecting application data, cloud providers also hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks.

Risk Management

Assessing and managing risk in systems that use cloud services can be a challenge. With cloud-based services, some subsystems or subsystem components fall outside of the direct control of a client organization. Many organizations are more comfortable with risk when they have greater control over the processes and equipment involved. Establishing a level of trust about a cloud service is dependent on the degree of control an organization is able to exert on the provider to provision the security controls necessary to protect the organization's data and applications, and also the evidence provided about the effectiveness of those controls. Ultimately, if the level of trust in the service falls below expectations and the organization is unable to employ compensating controls, it must either reject the service or accept a greater degree of risk.

Architecture

The architecture of the software and hardware used to deliver cloud services can vary significantly among public cloud providers for any specific service model. It is important to understand the technologies the cloud provider uses to provision services and the implications the technical controls involved have on security and privacy of the system throughout its lifecycle. With such

information, the underlying system architecture of a cloud can be decomposed and mapped to a framework of security and privacy controls that can be used to assess and manage risk.

Identity and Access Management

Data sensitivity and privacy of information have become increasingly an area of concern for organizations. The identity proofing and authentication aspects of identity management entail the use, maintenance, and protection of PII collected from users. Preventing unauthorized access to information resources in the cloud is also a major consideration. One recurring issue is that the organizational identification and authentication framework may not naturally extend into a public cloud and extending or changing the existing framework to support cloud services may prove difficult.

Software Isolation

High degrees of multi-tenancy over large numbers of platforms are needed for cloud computing to achieve the envisioned flexibility of on-demand provisioning of reliable services and the cost benefits and efficiencies due to economies of scale. Regardless of the service model and multi-tenant software architecture used, the computations of different consumers must be able to be carried out in isolation from one another, mainly through the use of logical separation mechanisms.

Data Protection

Data stored in a public cloud typically resides in a shared environment collocated with data from other customers. Organizations placing sensitive and regulated data into a public cloud, therefore, must account for the means by which access to the data is controlled and the data is kept secure. Similar concerns exist for data migrated within or between clouds.

Value Concentration

Having data collocated with that of an organization with a high threat profile could also lead to a denial of service, as an unintended casualty from an attack targeted against that organization. Similarly, side effects from a physical attack against a high profile organization's cloud-based resources are also a possibility. For example, over the years, facilities of the Internal Revenue Service have attracted their share of attention from would-be attackers.

Data Isolation

Database environments used in cloud computing can vary significantly. Accordingly, various types of multi-tenant arrangements exist for databases. Each arrangement pools

resources differently, offering different degrees of isolation and resource efficiency. Regardless of implementation decision, data must be secured while at rest, in transit, and in use, and access to the data must be controlled.

Data Sanitization

The data sanitization practices that a cloud provider implements have obvious implications for security. Sanitization involves the expunging of data from storage media by overwriting, degaussing, or other means, or the destruction of the media itself, to prevent unauthorized disclosure of information. Data sanitization also applies to backup copies made for recovery and restoration of service and residual data remaining upon termination of service.

In a public cloud computing environment, data from one consumer is physically collocated (e.g., in an IaaS data store) or commingled (e.g., in a SaaS database) with the data of other consumers, which can complicate matters. Service agreements should stipulate sufficient measures that are taken to ensure data sanitization is performed appropriately throughout the system lifecycle.

Encryption

Client end-to-end encryption (e.g., encryption/decryption occurs on the law enforcement controlled client prior to data entering the cloud and decryption occurs only on the client device after encrypted data is removed from the cloud service) with cryptographic keys managed solely by law enforcement would prevent exposure of sensitive data.

- May cause significant cloud service functionality limitations on available service types made available for sensitive data. This may also increase expenses to cover key items, such as key management and client software. Additionally, a number of specific SLA or contract clauses may be necessary for the implementation of client end-to-end encryption.

Use of cloud services without end-to-end encryption implemented by the client is another option that would require cloud service provider participation in the encryption of data.

- This would require at least some cloud provider personnel to undergo personnel background screening and training.
- Specialized Service Level Agreements (SLA) and/or contractual clauses would be necessary to identify those personnel that may have access to unencrypted, sensitive data.
- Conducting the analysis and gaining approval of particular cloud service implementations not utilizing end-to-end encryption for sensitive law enforcement data may be costly and time consuming due to the high degree of technical complexity.

Availability

In simple terms, availability is the extent to which an organization's full set of computational resources is accessible and usable. Denial of service attacks, equipment outages, and natural disasters are all threats to availability. The concern is that most downtime is unplanned and can impact the mission of the organization. Some examples of unplanned service interruptions that cause concerns are:

- Temporary Outages
- Prolonged and Permanent Outages
- Denial of Service

Incident Response

The complexity of a cloud service can obscure recognition and analysis of incidents. Revising an organization's incident response plan to address differences between the organizational computing environment and a cloud computing environment is an important, but easy-to-overlook prerequisite to transitioning applications and data.

Data Availability

The availability of relevant data from event monitoring is essential for timely detection of security incidents. Cloud consumers are often confronted with extremely limited capabilities for detection of incidents in public cloud environments. The situation varies among cloud service models and cloud providers. For example, PaaS providers typically do not make event logs available to consumers, who are then left mainly with event data from self-deployed applications (e.g., via application logging). Similarly, SaaS consumers are completely dependent upon the cloud provider to provide event data such as activity logging, while IaaS consumers control more of the information stack and have access to associated event sources.

Incident Analysis and Resolution

An analysis to confirm the occurrence of an incident or determine the method of exploit needs to be performed quickly and with sufficient detail of documentation and care to ensure that traceability and integrity is maintained for subsequent use, if needed (e.g., a forensic copy of incident data for legal proceedings). Issues faced by cloud consumers when performing incident analysis include lack of detailed information about the architecture of the cloud relevant to an incident, lack of information about relevant event and data sources held by the cloud provider, ill-defined or vague incident handling responsibilities stipulated for the cloud provider, and limited capabilities for gathering and

preserving pertinent data sources as evidence. Understanding and negotiating the provisions and procedures for incident response should be done before entering into a service contract, rather than as an afterthought.

General Recommendations:

A number of significant security and privacy issues were covered in the previous subsections. Table 1 summarizes those issues and related recommendations for organizations to follow when planning, reviewing, negotiating, or initiating a public cloud service outsourcing arrangement.

Table 1: Security and Privacy Issue Areas and Recommendations

Areas	Recommendations
Governance	<ul style="list-style-type: none"> Extend organizational practices pertaining to the policies, procedures, and standards used for application development and service provisioning in the cloud, as well as the design, implementation, testing, use, and monitoring of deployed or engaged services. Put in place audit mechanisms and tools to ensure organizational practices are followed throughout the system lifecycle.
Compliance	<ul style="list-style-type: none"> Understand the various types of laws and regulations that impose security and privacy obligations on the organization and potentially impact cloud computing initiatives, particularly those involving data location, privacy and security controls, records management, and electronic discovery requirements. Review and assess the cloud provider's offerings with respect to the organizational requirements to be met and ensure that the contract terms adequately meet the requirements. Ensure that the cloud provider's electronic discovery capabilities and processes do not compromise the privacy or security of data and applications.
Trust	<ul style="list-style-type: none"> Ensure that service arrangements have sufficient means to allow visibility into the security and privacy controls and processes employed by the cloud provider, and their performance over time. Establish clear, exclusive ownership rights over data. Institute a risk management program that is flexible enough to adapt to the constantly evolving and shifting risk landscape for the lifecycle of the system. Continuously monitor the security state of the information system to support on-going risk management decisions.

Areas	Recommendations
Architecture	<ul style="list-style-type: none"> Understand the underlying technologies that the cloud provider uses to provision services, including the implications that the technical controls involved have on the security and privacy of the system, over the full system lifecycle and across all system components.
Identity and Access Management	<ul style="list-style-type: none"> Ensure that adequate safeguards are in place to secure authentication, authorization, and other identity and access management functions, and are suitable for the organization.
Software Isolation	<ul style="list-style-type: none"> Understand virtualization and other logical isolation techniques that the cloud provider employs in its multi-tenant software architecture, and assess the risks involved for the organization.
Data Protection	<ul style="list-style-type: none"> Evaluate the suitability of the cloud provider's data management solutions for the organizational data concerned and the ability to control access to data, to secure data while at rest, in transit, and in use, and to sanitize data. Take into consideration the risk of collating organizational data with that of other organizations whose threat profiles are high or whose data collectively represent significant concentrated value. Fully understand and weigh the risks involved in cryptographic key management with the facilities available in the cloud environment and the processes established by the cloud provider.
Availability	<ul style="list-style-type: none"> Understand the contract provisions and procedures for availability, data backup and recovery, and disaster recovery, and ensure that they meet the organization's continuity and contingency planning requirements. Ensure that during an intermediate or prolonged disruption or a serious disaster, critical operations can be immediately resumed, and that all operations can be eventually reinstituted in a timely and organized manner.
Incident Response	<ul style="list-style-type: none"> Understand the contract provisions and procedures for incident response and ensure that they meet the requirements of the organization. Ensure that the cloud provider has a transparent response process in place and sufficient mechanisms to share information during and after an incident. Ensure that the organization can respond to incidents in a coordinated fashion with the cloud provider in accordance with their respective roles and responsibilities for the computing environment.

G.4 Mobile Appendix

Mobile Appendix

Introduction

Mobile devices present a unique security challenge with regard to the correct application of CJIS Security Policy requirements. This appendix is intended to provide best practices based on industry standards and on methods to achieve policy compliance in mobile device employment scenarios. The technical methods used to achieve compliance with CJIS Security Policy will typically be different within the mobile environment than those used in fixed locations. Many of the security features and capabilities inherited by endpoint devices from the fixed environment are either not present or present in a different form in the mobile environment. Additionally, the basic technologies used in some types of mobile devices may adequately fulfill some of the CJIS Security Policy requirements which would require additional software or added features in a traditional fixed computing environment. Due to the complexity and rapid evolution of the mobile environment, this Appendix will remain as device and vendor agnostic as practical, however certain key requirements for specific mobile operating systems will be identified for the major mobile operating systems (e.g., Apple iOS, Android) as the underlying technologies are fundamentally different and offer different levels of built-in compliance to CJIS Security Policy.

Sections within this appendix will provide recommendations regarding priorities and level of effort versus value of applying certain security controls in the mobile environment. These recommendations do not supersede or modify the requirements listed in the CJIS Security Policy, and are intended to describe the effect of inherent security functions and inherent device limitations in many mobile platforms that impact the application of policy elements in the mobile environment.

Mobile Device Risk Scenarios

There are multiple risk scenarios that may apply to mobile devices depending on the category of device (e.g., Laptop, Tablet, and ‘Pocket sized’ devices such as smartphones) and the methods of device connectivity (e.g., cellular service, Wi-Fi + Cellular, Wi-Fi only). Device category and method of connection define the technology types within the device which inherently affects the total level of compliance with CJIS Security Policy that can be obtained by the mobile device.

It is advisable for acquiring agencies to review the mobile device guidance in this Appendix prior to completing selection and acquisition of particular devices. Both the device category and connectivity methods installed and configured on the device will impact the overall risk scenario associated with the device and may significantly affect the effective cost to bring use of the device in compliance with the CJIS Security Policy. For instance, inclusion of cellular radios with the ability to remotely control a device significantly changes the risk scenario by allowing remote tracking, file deletion, and device management which could provide a higher level of CJIS Security Policy compliance than a Wi-Fi only device that does not guarantee the ability to remotely manage the device. However, inclusion of cellular technology may significantly increase the initial device costs and incur ongoing subscription costs. Appropriate choices based on the intended use of the

device along with the types and methods of Criminal Justice Information (CJI) data to be accessed could greatly reduce agency cost and enhance security.

Device Categories

This appendix defines risk levels for three categories of devices. Prior to reading individual sections of this Appendix, the agency should identify which device categories will apply to their employment scenario. If multiple categories of devices are employed, individual technical configurations and local policy will likely need to be defined for each category of device based on the risk inherent in the technical characteristics associated with each device category.

Laptop devices

The laptop device category includes mobile devices in a larger format that are transported either in a vehicle mount or a carrying case and include a monitor with attached keyboard. This includes all traditional laptop computers that utilize a ‘traditional’, full-featured operating system (e.g., Windows or a Linux variant). Also included in this category are ‘tablet’ type full-featured computers running a traditional full-featured operating system but without an attached keyboard. The main defining factor is the use of a full-featured operating system and a form factor too large to be carried in a pocket. In general, devices of this type connect via Wi-Fi only, but may include an internal cellular access card in some cases.

The risks associated with this device type are similar to a standard desktop computer at the technical level, but are increased due to the potential to connect directly to the internet without the benefit of organizational network security layers (e.g., network firewall, IDS/IPS, network monitoring devices). There is also an increased risk of intentional device theft from vehicles or unsecure locations as these devices are too large to be carried on the authorized user’s body. There may be increased risk from the limited technical ability to wipe or track a lost/stolen device depending on the particular technical means used for remote device connectivity (e.g., cellular or Wi-Fi).

In general, the technical configurations for compliance with most of the CJIS Security Policy that is accomplished via the operating system (e.g., auditing, access control, etc) will remain consistent with normal fixed location computing systems for laptop devices, but some functions may operate in an unexpected manner due to lack of constant connectivity. Thorough testing of applied security policy elements within the expected mobile environments will help ensure the applied policy configurations remain effective and appropriate when applied to mobile laptop devices.

NOTE: Some newer devices running multi-function operating systems (e.g., Windows 8 or similar multi-mode operating systems) may exhibit technical features associated with both laptop and tablet device categories based on their current operating mode which may be reconfigured by the user on demand. If this is the case, it will be necessary to assess and configure multiple operating modes to be compliant with CJIS Security Policy on the device, or restrict the operating mode to one category of operation.

Tablet devices

The tablet device category includes larger format devices transported via vehicle mount or portfolio sized carry case that typically consist of a touch screen without attached keyboard. These devices utilize a limited-feature operating system (e.g., Apple iOS, Google Android, Windows mobile) that is inherently more resistant than a traditional operating system to certain types of network based technical attacks due to the limited-feature sets. Additionally, limited functionality

operating systems are designed specifically for the mobile environment where battery life and power efficiency are primary design drivers. This inherently limits the types of services that can function effectively on the devices (e.g., traditional real-time anti-virus software) as the base operating system may not be designed to allow installed applications enhanced execution priority in the background and or the ability to examine the contents or communications associated within another application. However, this same design methodology significantly limits the vectors available for malware transmission and the device or application data actually accessible to malware if a device becomes infected.

Tablet devices will have different risks associated depending on the installed and configured methods for network access (e.g., ‘always on cellular’ vs. Wi-Fi only). Physical risks associated with this category are similar to the laptop category for enhanced likelihood of intentional theft or device hijacking while unattended, while the technical risks are similar to the pocket device category.

Pocket devices/Handheld devices

The pocket/handheld device category is technically similar or identical to the tablet category and is primarily differentiated by device form factor. Pocket/handheld devices are characterized as having a limited functionality operating system and a small form factor intended for carry in a pocket or ‘holster’ attached to the body. The bulk of this category will be cellular ‘smartphones’ with integrated cellular data connectivity, however devices intended to be worn or carried on the body (e.g., portable fingerprint devices) may also be included in this category if they operate using a limited functionality operating system. Custom or specialty devices may meet the form factor distinction for this category, but operate using a full-feature operating system. In rare cases of this nature the employing agency should apply security guidance and principles in this appendix for both the laptop and pocket device categories.

Risks associated with this category are a reduced threat of theft to a stored devices (e.g., device left unattended in a vehicle) since these devices are typically carried continuously by the authorized user, but include a greater risk of temporary or permanent loss of control due to the device being misplaced by the authorized user.

Due to the installation of a limited functionality operating system, the technical threat to these devices via a network based attack is significantly lower than the laptop category, however, the threat of unauthorized access at the device level may be higher if the device is lost due to technical limits on multi-factor authentication to the operating system itself and practical limits to device passwords due to screen/software keyboard limitations.

NOTE: Data accessible on pocket or tablet devices simply through the entry of a single device PIN or password should not be considered secure due to the likelihood of enhanced password guessing based on fingerprints/smudges on the device touch screen. Any data stored on devices of these types should be protected within a separate secure container using Advanced Authentication.

Device Connectivity

There are three main categories of device connectivity that are associated with varying risk levels and threats to the devices. The Three categories are: Cellular Network Only (always on), Wi-Fi Only (includes ‘on demand’ cellular), and Cellular (always on) + Wi-Fi network. The risks associated with connectivity categories are general risks and may apply differently to any particular device at different points in its usage or lifecycle. Particular device configurations either

through the operating system or a third-party mobile device management (MDM) system may be able to significantly control and define which particular connectivity risks may be associated with a particular device.

Cellular Network Only (always on)

Cellular network connectivity is characterized by ‘always on’ network connection through the device internal radio to a cellular network provider. There is a reasonable assurance that devices with ‘always on’ cellular can be tracked, managed, or wiped remotely if lost or stolen. This will significantly reduce risks associated with loss of the device and attempted illicit access to the device. One important consideration for this risk category is characterization of the device as ‘always on’ or ‘on demand’. In effect the difference is typically a configuration setting, which in some cases may be changeable by the user. In particular most cellular smart phones contain ‘airplane’ mode settings that disable all internal radios allowing a user authenticated to the device operating system via password or personal identification number (PIN) to disable the cellular system. Access to this functionality may be disabled through the use of some MDM systems which would necessitate a complete power down of the device while carried on aircraft. Additionally, someone illicitly obtaining a device with properly configured password requirements and screen lock timeouts would be unlikely to guess the device password before the device was reported stolen in order for them to disable the cellular connection and prevent tracking or a remote wipe of the device.

Cellular networks do not allow for the same level of exposure of individual devices to random access from the internet. This significantly reduces the potential network based attack vectors that might reach a cellular connected device. The risk scenario in most cases from a network based attack would be similar to a device protected behind rudimentary network defenses (e.g., standard firewall but NOT advanced intrusion detection/prevention) Cellular device communications cannot typically be accessed by other ‘eavesdropping’ devices physically close to them without significant specialized equipment and can be considered well protected against network attacks below the nation/state level of technical capability by the hosting technical infrastructure and technology inherent in the device. However, network based attacks that utilize connections initiated by the user device may still succeed over the cellular infrastructure. For this reason, the technical protections inherent in the cellular infrastructure provide limited protection against user/device initiated actions (e.g., web surfing on a cellular connected web browser). Therefore, the protections provided by always on cellular connections are primarily in the ability to remotely access the mobile device for tracking or data deletion in case of device loss or compromise, which combined with a limited functionality device operating system, the protections are generally equivalent to a ‘personal firewall’ if properly configured and supported by a well-designed organizational infrastructure. However, that equivalency does not apply to full-featured operating systems connected through cellular infrastructure.

NOTE: It should be noted that a technically capable, intentional, thief knowingly obtaining an ‘always on’ cellular device for the purpose of data theft can physically disable the radio by utilizing a Faraday cage or similar external electromagnetic shield device while attempting to guess the device password. While technically possible these methods require specialized equipment and high technical expertise and would be very unlikely to be employed except for specifically targeted attacks. When always on cellular connectivity is combined with a robust incident reporting process and user training for rapid response to device loss or theft, the associated risks can be minimized.

Wi-Fi only (includes 'on-demand' cellular)

Wi-Fi only devices do not include cellular radios or include cellular radio that must be manually activated or 'connected' to the cellular network. They connect to the network or internet through Wi-Fi 'hotspots' or external access points or manually to cellular networks. Some MDM or device configurations may be able to limit the types and specific Wi-Fi access points the device can connect to, which may change the risk scenario of the device to a similar risk scenario as the Cellular Network Only scenario. However, if mobile devices are permitted (through technical and or policy decisions) to connect to any Wi-Fi access point designated by the device user, the overall device risk scenario is high and the device may be accessible to a large number of potential network based attack vectors. Unrestricted Wi-Fi access is not recommended on any agency owned device, but must be assumed to exist on any personally owned device authorized to access CJI. Significant compensating controls may be needed to ensure devices accessing CJI over 'public' Wi-Fi access points are not susceptible to communications network eavesdropping, credential hijacking or any of the various potential man-in-the-middle attacks possible through access point spoofing. The communications security risks can be significantly mitigated by mandatory device configurations (e.g., MDM based policy) that only allow devices to connect to cryptographically verified agency controlled Wi-Fi access points.

Wi-Fi only or devices with 'on-demand' cellular access (e.g., user or event driven cellular access initiated from the device and not from a centralized management location) are significantly more at risk from data loss subsequent to device loss or theft as there is no guarantee the tracking or remote wipe can be initiated once the device is out of agency control. This can be mitigated by utilizing tracking/anti-theft products that require a periodic network connection to authorize access and perform automated device locking ('bricking') or remote wipe if network connections are not made within a specified period. Software of this nature is generally available for full-featured laptops but may not be available for limited-feature mobile operating systems.

Cellular (always on) + Wi-Fi Network

This is a hybrid scenario that has become typical with most 'smartphones'. These devices contain both the always on cellular connection, but may also be configured to access local Wi-Fi networks for enhanced bandwidth. In considering devices with these technical characteristics, the theft/loss risks are similar to the cellular only scenario (due to tracking and remote access through the cellular connection), while the data and network based risks must be considered to be similar to the Wi-Fi scenario unless the capability of the device to connect to Wi-Fi networks is limited by technology or policy to agency owned Wi-Fi Access Points configured in accordance with the CJIS Security Policy. Careful consideration must be made to the particular configurations, management systems, and human oriented operational policies based on the particular technical capabilities and configurations of these types of devices.

Incident Handling (CJIS Security Policy Section 5.3)

Additional or enhanced incident reporting and handling procedures will need to be developed to cover mobile device operating scenarios. Various exploits and methods to compromise mobile devices require either specialized equipment or lengthy operations to implement. Rapid response to mobile device related incidents can significantly mitigate the risks associated with illicit data access either on the device itself or within online data resources associated with the device through an application or specialized interface. However, parallel or special incident handling procedures with associated equipment or systems may need to be put in place to properly respond to incidents

involving mobile devices. This section lists three areas where enhanced incident handling and response processes may need to be implemented to ensure mobile device compliance to the incident handling policy in Section 5.3.

If personally owned devices are utilized within the environment in a Bring Your Own device (BYOD) scenario, specialized and costly incident handling procedures and processes may need to be developed to support compliance for those devices. The costs associated with enhanced incident handling procedures may need to be incorporated in the cost and risk based analysis to allow personally owned devices in the BYOD scenario, as the technical methods and risk to achieve compliance under BYOD scenarios may exceed any cost savings potentially achieved through BYOD.

Loss of device Control

Mobile device users should be trained and provided with explicit user actions in case positive control of a mobile device is lost for any period of time. Loss of positive control means the device is in the physical control of non-CJIS authorized individual or the device is left unattended in an unsecure location (e.g., counter of the coffee shop). Even if the device is recovered quickly there is significant risk that either the device settings could be tampered with or data on the device could be illicitly accessed. The level of detail and particular scenarios identified in the agency incident response plan should be consistent with the presence of persistent CJI on the device or the technical means used to access CJI from the device (e.g., ask the question: “Is it reasonable to assume CJI could be accessed”) as well as the degree of device configuration control exercised by the user from the device main login. At a minimum, special incident handling procedures should be developed for the following scenarios:

- Device known to be locked, control loss of minimal duration
- Device lock state unknown at time of control loss, duration of loss minimal
- Device lock state unknown at time of control loss, duration of loss extended
- Device known to be unlocked at time of control loss, duration of loss more than momentary.

NOTE: Organizations should define appropriate time value criteria based on the operational environment for the above scenarios. For instance, a ‘momentary’ loss of control might be considered a matter of seconds in a situation where no one could reasonably have accessed the device, while ‘minimal’ durations might include a few minutes of time and ‘extended’ periods would be any time longer than a few minutes.

Other scenarios should be addressed as appropriate to the intended device employment, with explicit user and organizational actions identified based on the device technologies and any organizational management capabilities.

Total Loss of device

Incident response scenarios for the total loss of the device should be developed based on the methods/storage of CJI on the device, the lock state of the device at time of loss (known locked, known unlocked, or unknown), and the technical methods available for remote tracking or wiping of the device. It is critical to implement incident handling procedures quickly in this case. Remote wipe functions can be implemented for always on cellular devices with a high potential for success that may include positive confirmation from the device that the wipe was completed. However, for

Wi-Fi only and on demand cellular devices, incident handling procedures that lock the device out of accessing CJI may be necessary, while there would be no guarantee that any CJI stored on the device could not eventually be accessed. For this reason, CJI should not generally be stored directly on Wi-Fi only or on-demand cellular devices unless an extremely robust anti-tamper system is in place on the device itself.

Potential device Compromise (software/application)

Incident response scenarios for potential device compromise through intentional or unintentional user action should be developed to ensure compliance with policy. This includes rooting, jailbreaking or malicious application installation on the device during a loss of device control scenario or inappropriate user action in the installation of applications to the device (compromise can occur from either intentional threat agent actions or accidental user actions). Triggers for this incident handling process may be driven from either user notification or electronic detection of device tampering from an audit or MDM compliance check.

Audit and Accountability (CJIS Security Policy Section 5.4)

The ability to implement some Audit and Accountability functions specified in the CJIS Security Policy on mobile devices with limited function operating systems (e.g., Android, Apple iOS) is not natively included within the operating system. Either additional device management systems, enterprise mobility management (EMM) or MDM, or auditing from systems accessed by the mobile device will be necessary to ensure appropriate levels of auditing exist.

Auditable Events (reference 5.4.1)

Some of the specific audit requirements in the CJIS Security Policy may not be technically relevant to the mobile operating system due to its internal functioning. To achieve compliance with the CJIS Security Policy it will be necessary in most cases to utilize some form of MDM or EMM system. Additional auditable events that compensate for the technical limitations of limited function mobile operating systems may be available through the use of MDM systems (e.g., association of event with global positioning system (GPS) location of the device). Specific auditable events of interest in the mobile environment will depend on the intended device usage, compartmentalization of data on the device, and options available with the specific technologies employed. For instance, item 2 in Section 5.4.1.1 indicates an auditable event includes attempts to modify elements of user account modification. Due to the limited internal functions of mobile operating systems, this event type is not relevant to the operating system itself as they are generally provisioned with only a single non-modifiable user account on the device. To achieve compliance in a scenario where CJI is stored or accessed from a secure application on the device, auditing of access to the secure application either through application design, or third party MDM capability may provide an acceptable compensating control. For compliance with the policy each auditable event and event content must be compared to the particular technologies and applications employed to determine if adequate compensating controls are being met for audit items that either do not apply to mobile technologies or cannot be implemented within the technology itself.

Alternative and compensating controls that provide detailed audit of access to CJI either on the mobile device itself or through a controlled application to a central server may provide equivalent auditing capability to the events specified in the policy. However, multiple auditing systems may be required to replicate the auditing provided at the operating system level by a full function operating system. Therefore, the overall auditing design should take into account retrieval and

consolidation of events or audit data from multiple auditing systems as appropriate to comply with policy.

Audit Event Collection

Mobile devices without an ‘always-on’ cellular connection may pose technical challenges to ensure any audit records collected and stored on the mobile device itself can be retrieved for review and analysis per the CJIS Security Policy. Alternatively systems which explicitly require a network connection to a central server to access data or decrypt on-device storage may provide acceptable audit event collection and reporting since there is a guarantee that network connections must be in place for CJI to be accessed. Careful consideration should be made regarding the accessibility of audit records when developing the mobile audit scheme.

Access Control (CJIS Policy Section 5.5)

Access control associated to limited functionality mobile operating systems will typically operate in a different manner than full function operating systems. For instance there is normally not a provision for multiple user accounts on many mobile operating systems which may mean the policy requirements for access control (e.g., regarding account management) would not be apply to the mobile operating system, but should rather be applied to a particular application, either stand-alone to the device or as part of a client server architecture. Application of access control policy identified in the CJIS Security Policy will often need to be applied to elements of the total system beyond the device operating system.

For example, CJI stored or accessed from a secure mobile application that requires connectivity to a CJIS authorized server architecture could potentially accomplish most or all of the access control policy elements based on user authorization via the secured application and be largely independent of the mobile operating system. Alternatively, if storing CJI in ‘general’ purpose data storage containers on a mobile device it may not be possible to achieve compliance with the CJIS Security Policy. Careful consideration and deliberate design of mobile applications or data storage will be required to achieve compliance on mobile devices.

Due to the inherent nature of limited function mobile operating systems, very tight access controls to specific data is actually implemented within the operating system. This effectively prevents applications from accessing or manipulating data associated with other applications to a very high degree of confidence as long as the device is not rooted or jailbroken. However, the device user is automatically granted access to all device data through the associated application unless the application itself has a secondary authentication and access control methodology. Additionally, since basic device functions (e.g., phone) are typically protected using the same password or PIN as the device level encryption, use of a weak PIN to allow easy access to basic device functions largely negates the value of the integrated device encryption.

If personally owned devices are utilized within the environment (BYOD scenario), specialized and costly access control methods may be required to reach compliance with CJIS Security Policy. The costs associated with enhanced access control procedures and technologies should be incorporated in the cost and risk based analysis to determine whether or not to allow personally BYOD, as the technical methods and compensating controls required for CJIS Security Policy compliance are likely to exceed any potential cost savings for implementing BYOD.

Device Control levels and access.

Limited function mobile operating systems are typically very constrained on the levels of access provided to the user. However, intentional user actions (e.g., installing an application and accepting inappropriate security access levels for that application) may bypass some of the built in security protections inherent in the limited functionality devices. Compliance with CJIS Security Policy may be difficult without the addition of strict device control policy. In a mixed environment (e.g., agency owned devices and BYOD), access control policy with BYOD systems may be impractical or impossible to fully implement.

Embedded passwords/login tied to device PIN.

Limited function mobile operating systems typically allow the association of multiple passwords and access credentials with particular applications. The system access provided by these embedded credentials will often be tied to the device password or PIN. An example would be access to device integrated email and calendar applications. Alternatively a 'corporate' email application may independently encrypt the data associated with the application and require a separate login from the device itself. Access to CJI utilizing only the device level password or PIN and device embedded credentials is not compliant with CJIS Security Policy unless protected with Advanced Authentication, which is not currently possible on most devices. Therefore, use of integrated device functions (e.g., built in email or chat) to store or transmit CJI would also not be compliant.

Access requirement specification

In general, due to weaknesses associated with password guessing based on analysis of fingerprints or swipes on the device touch screen, short (4-8 digit) device PIN numbers provide limited security to a determined password guessing attack. Conversely, utilization of a robust password at the device level may be inconsistent with quick access to basic device functions (e.g., phone). When developing specific CJIS compliant access control and authentication schemas a layered approach with the device PIN protecting only the basic device functions (e.g., phone, camera, non-secure applications) and a more robust password or multifactor authentication used to protect applications or data storage may achieve policy compliance where the device password/PIN would not. In a layered security deployment, careful attention must be placed on the capability to share data (e.g., cut and paste or screenshot functions) between secure applications with CJI or CJI access and basic device functions with limited security controls.

Special Login attempt limit

Depending on the access and authentication scheme applied to the mobile device, it may be appropriate to fully comply with the CJIS login attempt limits within a secure application or container and not solely at the device level. However, the device itself should have login attempt limits consistent with the risk associated to the data or configurations accessible on the device itself. Since mobile devices are inherently portable, and can easily be removed from a location. Brute force attempts to gain access to the system, especially when protected only by a short PIN, are likely to be successful given sufficient time. Special consideration should be made based on device connectivity methods (cellular, Wi-Fi, etc) on the appropriate number of unsuccessful login attempts that will be allowed and the resultant actions taken by the device. Most devices either natively allow for the device to wipe itself after a failed number of attempts, or allow the application of EMM/MDM applications to perform wiping actions after a predetermined number of failed login attempts.

Login failure actions

Mobile devices with or without MDM software can typically be configured to perform actions based on serial unsuccessful login attempts. Appropriate actions to configure may be dependent on the data resident on the device and the connectivity method employed by the device. Most devices can be configured to delete all data on the device and/or issue an alert to the network if a number of incorrect passwords are entered. This is a very advantageous feature, however specific configuration of the number of attempts and resultant action must be considered against the state of the device after an unsuccessful attempt action is triggered. A full device wipe will typically leave the device in a fully or partially non-functional state which could introduce risk if part of the intended use is time critical phone calls. Where possible, full device wipe associated with unsuccessful attempts at the device level password should be configured but the number of invalid attempts may exceed the CJIS Security Policy at the device level if all CJI on the device is protected by an additional layer of encryption protected by a subsequent secure application authentication method that is technically prevented (via complexity rules or entry rules) from being the same as the device level authentication and the secure application is configured in accordance with the policy and also contains a secure data wipe capability after a specified number of incorrect authentication attempts.

System use Notification (CJIS Policy reference 5.5.4)

Agency policy should include specific mandatory language consistent with the CJIS Security Policy to identify the device restrictions and consent. However, due to screen size limits, some mobile devices may not be technically capable of displaying the full text used with traditional operating systems. To achieve compliance agencies should contact their legal department for appropriate wording of a short version of the system use notification that can be set to display within the constraints of the device lock screen. This may be accomplished through embedding the text into an image displayed on the lock screen or some other external device labeling method if the device does not permit sufficient text to be displayed.

In a BYOD environment or mixed (agency owned and BYOD), it may be necessary to develop or deploy custom applications that can achieve compliance with the system use notification upon access and prior to any CJI access being allowed.

Session Lock (CJIS Policy reference 5.5.5)

Due to the portable nature of mobile devices the session lock limit in the general CJIS Security Policy may be excessive in the mobile environment for certain device functions and insufficient for other functions based on intended device usage. Agencies should examine the minimum lock time practical for all mobile devices based on their employment scenario and ease for which a user can manually lock the device. The actual session lock times should be adjusted as appropriate to the device type, device operational location, and the data accessible on the device when unlocked. Pocket size devices are at greatest risk if screen lock times are insufficient, however, for devices used in emergency response or communication, extended lock times at the basic device level may be considered if CJI is subsequently protected by an application or web interface utilizing more stringent secure locking functions. A well designed solution may include multiple session lock settings at the device and individual application levels to ensure the CJIS Security Policy requirements are met for CJI access, while other device functions are accessible under different session lock configurations.

Device Wi-Fi Policy

Specific Wi-Fi configuration policy should be developed based on the intended use environment and data access requirements for the device. The policy should explicitly cover configuration of device connections. Technical methods specific to the mobile technologies may need to be implemented to ensure all mobile devices are compliant with CJIS Security Policy. Current CJIS Security Policy provides detailed configuration requirements for Wi-Fi connections, however it was originally intended for defining requirements for fixed infrastructure Wi-Fi (802.11) supporting wireless within a facility. The security requirements identified for fixed infrastructure installations are applicable to mobile usage, however there are several mobile specific scenarios where the requirements may not be clear. The following sections identify areas not specifically covered in the existing policy that will require special handling to ensure wireless connections are compliant.

Hotspot capability

Many mobile devices now include the capability to activate an internal Wi-Fi hotspot that allows other devices to connect through the hosting device to the internet over the devices cellular radio. While this is a potentially valuable capability when multiple law enforcement devices may need localized internet or network access, mobile hotspots should be configured as consistent with the CJIS Security Policy on wireless access points. Connections must only be accepted from known and approved devices in order to protect the integrity of the hosting device as well as the communications security of other connected devices. Since most mobile hotspots are not technically capable of providing the device authentication required for infrastructure wireless, use of mobile hotspot capability should assume the overall portable Wi-Fi network itself is not secure and CJI should not be transmitted or exposed on the network without appropriate encryption.

Connection to public hotspots

There are significant risks to connecting to public wireless access points. Rogue access points masquerading as legitimate public access points may allow for man-in-the-middle, eavesdropping, and session hijacking attacks. While not specifically prohibited in the current CJIS Security Policy, it is recommended that connection to public internet access points be technically restricted by device configuration or MDM systems if possible. CJI access mechanisms from mobile devices should include robust authentication methods specifically designed to prevent interception or hijacking of CJI or user information through the use of a rogue access point masquerading as a legitimate public wireless access point. Transmission encryption alone may not provide sufficient protections when device connections originate at public hotspots. Since the public hotspot controls access to all network services at the connection point (e.g., Domain Name System) attacks against the transmission path are possible that would not normally be feasible in a fixed environment where communications exist between two secured network enclaves.

Cellular Service abroad

If mobile devices are used outside of the United States, especially if connected to foreign cellular networks, specific handling procedures may need to be developed for the use of the device while abroad and the assessment or configuration check of the device state once the devices are returned to the United States. Certain device internal functions on cellular devices may be modified or compromised by the cellular carrier as the devices are intended to have certain parameters configured by the cellular service provider which is considered a 'trusted' entity by the device.

Cellular carriers within the United States are constrained by United States laws regarding acceptable modifications to devices. Similar legal constraints cannot be assumed to exist in some areas of the world where laws and regulations for data and personal privacy may allow cellular carriers significantly more leeway in changes made to devices on their networks.

Security plans involving cellular connected devices that will be connected to foreign cellular networks should include technical and policy controls to ensure device use while abroad, data resident on the device while abroad, and the software integrity of the device once returned to the United States are all appropriate to the specific device and threat levels associated with the expected foreign travel. This should explicitly include considerations for devices in which an internal subscriber identity module (SIM) card is inserted into the device to obtain Global System for Mobile (GSM) cellular connections abroad to ensure any residual data on the SIM card is properly purged. Additionally, incident handling procedures may need to specify more stringent responses to even momentary loss of device control, and it may not be possible to assume tracking, anti-theft, and remote data wipe functions that work in the United States would be functional in all potentially visited geographic and political regions.

Bluetooth

Mobile devices utilizing Bluetooth should be evaluated for their ability to comply with the CJIS Security Policy Bluetooth requirements prior to acquisition. This includes the data device itself and any authorized Bluetooth accessories which will be associated to the device. While the technical security in current versions of Bluetooth is significantly stronger than legacy versions, mis-configuration of devices can still pose a significant threat in the mobile environment. If not specifically utilized for a required purpose, it would likely be most cost effective to disable or restrict the device Bluetooth radio utilizing device configurations or an MDM product. Additionally, the using agency may need to develop technically extensive training or user awareness programs to ensure use of Bluetooth capability does not render the device out of compliance if device users have the ability to make Bluetooth associations to the device. Specific instructions or guidance for specific devices could be developed to ensure all implementations are compliant.

Voice/Voice over IP (VoIP)

Cellular voice transmissions are distinctly different at the technical level than Voice over IP (VoIP) transmissions using voice/video applications (e.g., FaceTime, Skype). The use of VoIP is not specifically granted the exemption identified in CJIS Security Policy Section 5.5.7.3.2. Agencies wishing to use capability of this type should ensure the specific technical implementation complies with the Policy on authentication and data encryption.

Chat/Text

Device integrated chat/texting applications and many common third party chat applications authenticate and are identified using embedded passwords or the device identifier only. These functions should not be considered secure or appropriate for transmission of CJI data. Texting functions that utilize a cellular service providers Short Message Service (SMS) or Multimedia Messaging Services (MMS) functions do not constitute a secure transmission medium. Third party applications utilizing appropriate encryption and authentication methods independent of the device password/PIN may provide a compliant solution where the device integrated utilities are will not provide a compliant solution.

Administrative Access

Local administrative access to the mobile device, regardless of device category should be restricted by some mechanism. For traditional operating systems, configuration of a separate administrative account other than that used for normal logins to the device is an acceptable method to ensure appropriate access permissions to the mobile user for which they are authorized. However for limited functionality mobile operating systems (e.g., Android, Apple iOS) internal permissions and accounts assume a single authorized device user with explicitly defined permissions. Those permissions may be modified through policy applied to the device, but are typically global to the device itself. As a result, to ensure appropriate separation of access permissions, it may be required to ensure specific applications or software on the device are configured with individual authentication methods to separate application data from ‘general user’ access. Without additional authentication at the application level, access to specific application data would be available to any user with the ability to unlock the device. This may be appropriate in some scenarios with a high degree of assurance that the device can only be accessed by a single user, but sufficiently stringent device passwords and short screen lock times may prove problematic for practical use of some device functions. An alternate method to ensure strict separation of ‘routine’ device functions which may be accessed by multiple individuals (e.g., phone function if loaned to someone for a critical call) is to ensure any method used to access or store CJI has a separate and more stringent authentication method configured with rules that make it impossible to use the same authentication credential (e.g., PIN/Password) on both the device authentication and the application or function with access to CJI.

Rooting/Jailbreaking

‘Rooting’ (Android OS) or ‘Jailbreaking’ (Apple iOS) refer to intentional modifications to the mobile device operating system in order to grant the device user or an installed application elevated control that would not normally exist on the device. The security model internal to the various mobile device architectures vary significantly, however the common effect of rooting or jailbreaking the devices is to bypass many or all of the built in security features. The security feature bypass may be universal to all device features and installed applications once completed. Intentionally rooting or jailbreaking mobile devices should be avoided in any scenario as it potentially defeats all built-in data access and segregation controls on the device. Additionally the rooting or jailbreaking process itself has a heightened risk of introducing malicious code as part of the process, and also substantially increases the risk for malware to infect the device through user action. Extreme caution should be used if software is being installed that requires the devices to be rooted or jailbroken for the software or application to function. This is inclusive of purported security software that requires a rooted or jailbroken device to function. For example, on both the Android and Apple iOS platforms, the built-in security features for data access and memory segmentation prevent the effective operation of ‘traditional’ anti-virus and intrusion detection/prevention software. Software or applications purporting to perform these functions but requiring rooting or jailbreaking of the device and may actually accomplish the anti-virus or IDS/IPS function but are also likely to significantly increase the overall risk associated to the device by effectively disabling most or all of the integrated security features. A careful risk-based assessment should be conducted by a trained security professional prior to allowing the operation of any rooted or jailbroken mobile devices regardless of intended use. Significant compensating controls would be required to return a rooted or jailbroken device to minimal compliance with most of the CJIS Security Policy and would likely not be a cost effective approach.

NOTE: There is a distinction between rooting a ‘stock’ Android installation vice the installation of a separately supported secure operating system. There are secure versions of Android available or that can be developed based on the open source Android source code and compiled for installation on a particular hardware device. Installation of a secure, supported mobile operating system that replaces the device original operating system may significantly enhance the security of the device and should not be confused with ‘rooting’ and Android installation. Due to the close integration of operating system security with hardware elements, and the proprietary nature of Apple source code, there are not currently separate ‘secure’ versions of the Apple iOS and it is unlikely they will be developed.

Identity and Authentication

Due to the technical methods used for identity and authentication on many limited functionality mobile operating systems, achieving compliance to CJIS Security Policy may require layering of identification and authentication mechanisms. With the complexity and large number of potential identity and authentication solutions in the mobile environment emphasis must be placed on designing secure identity management and authentication architecture prior to the selection of individual devices or applications. Failure to consider a robust identity and authentication scheme as part of system design or acquisition will significantly increase the risk of subsequent noncompliance with CJIS Security Policy and potential added costs for a remedial solution. Many identity and authentication schemes used by existing commercial applications may make claims that appear to be consistent with CJIS Security Policy Advanced Authentication requirements, however, extreme care must be taken to ensure the actual technical implementation is compliant with policy.

Utilizing Unique device Identification

Some commercial applications and features integrated with some mobile operating systems permit the mobile device to be uniquely identified in a cryptographically robust manner. Any authentication schema that considers the possession of the mobile device as a factor in uniquely identifying and authenticating a CJIS authorized user must also include factors beyond than mere possession of the device. Larger form factor devices that cannot be carried on the person of the authorized user should not rely on possession of the device as an identifying factor, but may still include identifying capability within the device to provide assurance that the device itself is an authorized device. This should still be coupled with multi-factor advanced authentication to the device itself or the application hosting CJI. Coupling unique device authentication with robust advanced authentication of the user provides a high degree of confidence that both the specific device and the operator of the device are correctly identified. Utilizing device unique identification in order to authorize initial connections from the remote device back to the CJI hosting system or enclave provides additional protection to the CJI hosting system to reduce the attack surface of the hosting system and should be considered a good practice, but not in itself an authentication mechanism for the device user.

Certificate Use

One method for uniquely identifying mobile devices is to place part of a public key pair on the device in the form of a public key certificate. While there is value to ensuring the device itself can authenticate to a system supplying CJI, and may provide a critical layer of identification or authentication in a larger scheme, a certificate alone placed on the device should not be considered valid proof that the device is being operated by an authorized CJIS user, only that the device itself is authorized to host CJIS users. Additional user identification and authentication should be used to supplement any device certificate installed. Using a PIN or password separate from the device login to 'unlock' the certificate from cryptographic storage within a secure application will provide an additional layer of security and may increase the confidence level the device is being used by the intended user. However, use of public/private key pairs or pre-shared encryption keys can be utilized as part of an architecture to protect against certain session hijacking or man-in-the-middle attacks a mobile device may be susceptible to if connected to public internet connections.

Certificate Protections

Any certificates or cryptographic keys stored on any mobile device should include protections against the certificate or key being extracted from the device. Additionally certificates or other keys stored on mobile devices that grant the device special access or unique identification should be configured for remote wipe on demand or self-deletion based on a number of unsuccessful login or access attempts. Alternatively, methods may be used to revoke or invalidate the unique certificate or keys associated with a device.

Minimum Password/Pin (Reference CJIS Security Policy Section 5.6.2.1)

The minimum password protections identified in the CJIS Security Policy may not be appropriate for the device PIN/password due to immediate access requirement for some device functions (e.g., phone function) secured by the device PIN/password and the difficulty to enter a complex password under emergency conditions on a small screen. In cases where the risk of a complex password on the device itself is deemed significant, a layered authentication approach may be necessary where CJI or access to CJI is protected via one or more additional layers of access control beyond the device PIN/password. In cases where the CJI or access to the CJI is cryptographically segregated from applications accessible using the device level PIN/Password (e.g., secure application or secure browser vice the built-in browser) the authentication mechanism for the secure application or browser may satisfy the CJIS Security Policy requirements if fully compliant as a stand-alone application.

Configuration Management

Due to the potential for inconsistent network access or monitoring capability on mobile devices, methods used to monitor and manage the configuration of traditional full-featured operating systems may not function properly on limited function mobile operating systems. Configuration Management systems in the mobile environment may be designed in order to duplicate some of the functions typically performed by traditional anti-malware systems that will not function properly on some mobile operating systems.

Mobile Device Management (MDM)/Enterprise Mobility Management (EMM)

MDM and EMM systems and applications coupled with device specific technical policy can provide a robust method for device configuration management if properly implemented. MDM capabilities include the application of mandatory policy settings on the device, detection of

unauthorized configurations or software/applications, detection of rooting/jailbreaking of the device, and many other security policy related functions. In many cases, the most cost effective way to achieve CJIS Security Policy compliance on mobile devices is the selection of MDM or EMM applications and infrastructure appropriate to the mobile operating systems and intended access to CJI on the mobile devices. MDM/EMM functions may be applicable to most of the CJIS Security Policy requirements and allow for significant compensating controls in areas where traditional methods of CJIS Security Policy compliance are not technically feasible. Section 5.5.7.3.3 of the CJIS Security Policy specifies the minimum functions required for MDM. However, careful selection of the MDM product will potentially provide a cost effective method for additional areas of compliance in the access, auditing, incident response, authentication, media protection and system integrity sections of the CJIS Security Policy.

Device Backups/Images

Device images and backups provide protection against data loss, but also provide a method to quickly recover a device after damage or potential compromise. Due to an inherently limited ability to access the internal file structure of mobile devices, it can be difficult to easily identify a device compromise or illicit modification of the device. Some device imaging and assessment software may provide a secondary forensic capability, especially if there is intent for the device to be used outside the United States.

Bring Your Own device (BYOD) employment

BYOD environments pose significant challenges to the management of secure device configurations. In many cases it may be impossible to apply effective security that is acceptable to the device owner or it may require extremely costly compensating controls to allow access to CJI on personally owned devices. While allowed by the CJIS Security Policy, agencies are advised to conduct a detailed cost analysis of the ancillary costs of compliance with CJIS Security Policy on personally owned devices when they are approved for use. In some cases, a BYOD user may agree to abide by the same device configurations and limitations as imposed on an agency owned device, but signed user agreements should still be in place to ensure the agency has a legal right to recover or clear the device of all data prior to device disposal or employee termination. In other cases, robust secure applications may provide acceptable levels of compliance in a BYOD environment for limited CJI access but application design and architecture should assume the device itself is un-trusted. If MDM/EMM software capable of detecting rooting or jailbreaking of the device is not installed, any CJIS or data access occurring from the device is at a substantially higher risk of compromise.

Configurations and tests

Common configurations specific to all employed mobile devices should be developed to ensure compliance. Configuration tests should be developed and executed on all versions of mobile devices under all possible connectivity scenarios to ensure CJIS Security Policy compliance under all expected operating conditions. Since mobile devices can expect to operate in different physical and network environments, testing and validating correct security functions is more critical than on fixed computing platforms. Additionally, security functions that function properly on one version of a mobile operating system on a particular device may not function in the same manner even on the same version on a different device or a different version on the same device.

Media Protection

Some mobile device hardware platforms include the ability to add removable storage in the form of memory cards. This function is primarily related to Android and Windows mobile platforms and is intentionally limited on Apple devices, but may be possible through certain application functions. While the Android platform performs robust cryptographic separation of data stores between applications within the ‘internal’ storage of the device, the Android OS does not provide secure separation of data stores on ‘external’ storage. Some Android hardware devices include additional storage hardwired inside the device that is classified by the operating system as external storage and the normal separation between applications accessing that storage is not applied. Each potential device considered for acquisition must be assessed regarding specific ‘external’ media protection requirements which may actually include built-in media or storage.

Protection of device connected media

As a result of the limited protection and encryption capabilities applied to device removable media and SIM cards for cellular provisioning that include onboard data storage, all externally removable media or memory should be handled consistently with the CJIS Security Policy on media protection.

Encryption for device media

While most mobile operating systems have the capability to encrypt internal storage, it may require specific device settings to be enabled. All mobile device storage should meet the encryption requirements identified for media in the CJIS Security Policy. Specific settings may need to be applied to ensure proper encryption is actually employed. Additionally, the device built-in encryption capability is typically tied to the device PIN or password. Depending on the device PIN or password requirements the integrated encryption may be easily bypassed by password guessing and appropriate consideration should be made to ensure additional encryption protected by advanced authentication methods be applied to all CJI.

Physical Protection

Due to small form factors and the fact that mobile devices are often stored in lower security areas and vehicles, physical protection of the devices must be considered in both policy and training. Physical protections will often be the responsibility of the assigned device user and physical protections typically inherited by individual information systems from a secure facility will not be available to mobile devices which will require compensating controls to achieve compliance.

Device Tracking/Recovery

MDM software as well as some integrated mobile operating system functions may allow tracking of stolen or lost devices via ‘always-on’ cellular data connections and the devices built-in GPS. Device tracking with Wi-Fi only or ‘on-demand’ cellular access may not be reliable. Enabling device tracking capabilities, while not a replacement for secure storage, could be a compensating control used to substantially reduce overall device risk in some scenarios. Device tracking is not currently required in the CJIS Security Policy but should be applied to agency owned devices where possible as a risk mitigation factor. Enabling of device tracking on personally owned devices in a BYOD environment may raise employee privacy concerns and should be considered only for critical systems with the full knowledge of the employee and concurrence of the legal department. This is an enhanced risk that must be accepted for BYOD employments and should be considered

when allowing BYOD employment. Device tracking is available for both limited function mobile operating systems as well as traditional operating systems installed on laptop devices.

Access to device tracking software or applications within the organization should be controlled with limits and formal processes required to initiate a tracking action. It is advisable to include appropriate clauses in user agreements under what conditions and controls the organization applies to device tracking.

Devices utilizing unique device identification/certificates

Devices utilizing unique device identification or have installed certificates may require additional physical protection and/or additional incident handling steps in case of device loss in order to ensure the device unique identifier or certificate is immediately revoked or disabled. Additional physical protection rules or policy would be appropriate for any device which contains access mechanisms tied to the device.

System Integrity (CJIS Policy Section 5.10)

Managing system integrity on limited function mobile operating systems may require methods and technologies significantly different from traditional full-feature operating systems. In many cases the requirements of Section 5.10 of the CJIS Security Policy cannot be met with a mobile device without the installation of a third party MDM or EMM application and supporting server infrastructure.

Patching/Updates

MDM software may provide compliance to the Section 5.10.4.1 patch management requirements for particular platforms and software versions. However, devices without ‘always-on’ cellular connections may not be reachable for extended periods of time by the MDM or EMM solution either to report status or initiate patching. Supplementary or manual device accountability methods may need to be implemented to account for devices without persistent connections to ensure their patch and update state is current. Alternatively, some patches or system updates may not be practical over cellular connections and will require connection of devices to a Wi-Fi network. Compliance with CJIS Security Policy requirements through purely technical means may not be practical and considerations should be made for aggressive management of devices through training and mandatory periodic connection of devices to organizationally managed Wi-Fi networks.

TECHNOLOGY NOTE: Apple and Android based devices have different potential issues regarding device operating system updates. Apple maintains support for updating the operating system on Apple hardware for several device generations (typically 3-5 years) and provides a robust mechanism for system updates. However, updates to Android based systems are driven by the individual device manufacturer which may or may not support regular updates to current Android operating system versions. Additionally, different Android device vendors may offer updates/upgrades to the Android operating system on different schedules, which can complicate environments utilizing Android devices from multiple manufacturers.

Malicious code protection/Restriction of installed applications and application permissions

MDM or EMM software will typically allow restrictions on installed applications. One of the few effective attack vectors to compromise mobile operating systems is to manipulate the device user to install a malicious application. Even though the application may be restricted from accessing

other application data, it may have some access to common data stores on the device and access to device functions (e.g., GPS, microphone, and camera) that are undesirable. Unrestricted installation of applications by the device user could pose a significant risk to the device.

Malicious code protection using traditional virus scanning software is technically infeasible on most limited function mobile operating systems that are not rooted or jailbroken. The integrated data and program separations prevent any third party installed program from accessing or 'scanning' within another application data container. Even if feasible, power and storage limitations would be prohibitive in the effect on device battery life and storage capacity on most mobile devices. However, the cryptographic separation between applications and effective application virtualization technologies built into common mobile operating systems partially compensate for the lack of traditional virus scanning technologies. Appropriately configured MDM software is capable of checking the installed applications on the device and reporting the software inventory to a central management console in a manner analogous to traditional virus scan detection of unauthorized software. This behavior is analogous to the software inventory performed by anti-virus products and can provide a high degree of confidence that only known software or applications are installed on the device. While it is theoretically possible to bypass the application sandboxing and data segregation protections to compromise a mobile device through the web browser, the attack methods required are significantly more advanced than those required for a traditional full-featured operating system. Malicious code protections on the device web browser can be enforced through the use of a properly protected web proxy which the device is configured to use as a mandatory device policy. The most common method of malicious code installation is enticing the user to manually install the malicious app which can be mitigated on organizational devices using an MDM or other application installation restrictions which prevent the user from installing unauthorized or unknown applications. Mitigation of this issue within BYOD environments may not be possible and will present a significantly enhanced risk to the device.

TECHNOLOGY NOTE: In the particular area of application installation there is a significant difference between the behavior of Apple iOS and Android platforms. Apple cryptographically restricts the way applications will execute on the device and assigns mandatory application permissions when the application code is signed prior to release on the Apple App Store for distribution. Apps on the Apple platform must conform to Apple's policy on app behavior and cannot exceed their design permissions on access to common device functions once the app has been signed and distributed. However, the Apple method does not typically advertise the precise internal permissions granted to the app to the user prior to installation. At runtime, the app is required to request user permission to access certain device functions, and the user may agree or not agree, which may introduce risk if they are unaware of what they are agreeing to allow. Unsigned or un-trusted apps are cryptographically prevented from executing on non-jailbroken iOS devices. Apple provides a mechanism for organizations to distribute custom apps within an organization with equivalent protections but all receiving devices must have a special certificate installed that will only allow official App Store and the organization custom apps to execute.

Conversely, the Android platform, while also requiring app code signing, allows for self-signed code which can be distributed by means other than an official app store and execute on any Android device. Application permissions are presented to the user once at app installation but ramifications of agreement to certain app permissions may not be obvious to a non-technical user. Permissions in the Android model require user acceptance of all app requested permissions or the app is denied

installation, which can result in unwise user acceptance of excessive permissions in order to gain functionality provided by the app.

On either platform user installation of applications can significantly change the security state of the device. Applications may be able to transmit and receive data or share device common data with other devices over the network or local Wi-Fi or Bluetooth connection. On either platform it is highly desirable to limit allowable applications to a pre-approved pool of apps via MDM or organizational App store structures and device policy. However, the risks associated with uncontrolled app installation is several orders of magnitude greater on Android based devices.

WARNING: Rooted or jailbroken devices are modified in such a manner that the built in protections against malicious code are effectively disabled. A rooted or jailbroken device would require significant and costly compensating controls to achieve compliance.

Firewall/IDS capability

Traditional device or “personal” firewalls as identified in CJIS Security Policy Section 5.10.4.4 may not be practical on limited function mobile device operating systems but significant compensating controls are available. By default, mobile device operating systems have a limited number of system services installed and carefully controlled network access. To a certain extent the mobile operating system performs similar effective functions as a personal firewall would perform on a general purpose operating system. Potential compensating controls for the five (5) personal firewall requirements specified in Section 5.10.4.4 are listed below:

1. Manage Program Access to the Internet: On agency controlled devices with an MDM, limiting the apps installed on the device will effectively perform the same function. Since no software or apps can be installed without MDM approval a robust approval process can effectively ensure internet access is only granted to approved apps. Built-in apps and functions can also be limited on network access by the MDM.
2. Block unsolicited requests to connect to the user device: Default configurations for mobile operating system platforms typically block incoming requests. It is possible to install an app that may ‘listen’ on the network and accept connections, but the same compensating control identified in item 1 will mitigate the likelihood of that occurring.
3. Filter incoming traffic by IP address or protocol: Protocol filtering effectively occurs due to the limited function of the operating system as long as no installed application opens network access ports. The mitigations in 1 effectively compensate for this control as well.
4. Filter incoming traffic by destination ports: Same as 3.
5. Maintain an IP traffic log: This may not be technically feasible on most mobile operating system platforms as maintaining this log would require access to lower level operating system functions that are not accessible unless the device is rooted or jailbroken. However, individual Apps that communicate over the network or accept connections from the network may permit logs of IP traffic associated to that application to be stored.

Spam Protection

Spam guards installed on corporate or organizational email systems may effectively accomplish the spam protection requirements for the CJIS Security Policy on mobile devices if properly configured to block spam before delivery to the device. If no upstream spam guard is installed on the mail server the mobile devices accesses, the device may not have adequate spam protection. Additionally access to internet based email (web mail) would need to be restricted to web mail with appropriate spam and/or antivirus protections to ensure compliance.

Periodic system integrity checks

One method to compensate for the technical infeasibility of traditional anti-virus and malicious code protection is to install an MDM that performs periodic system integrity checks that validate device configuration and status against an approved baseline. Deviations may provide indicators of potential device compromise or mis-configuration.

G.5 Administrator Accounts for Least Privilege and Separation of Duties

Administrator Accounts for Least Privilege and Separation of Duties

PURPOSE:

This appendix is provided to describe industry best security practices for assigning separate administrator accounts to support the concept of Least Privilege.

ATTRIBUTION:

- SANS, “The Critical Security Controls for Effective Cyber Defense”, version 5.0
- NIST SP 800-53, “Security and Privacy Controls for Federal Information Systems and Organizations”, Revision 4 dated April 2013
- NIST SP 800-12, “An Introduction to Computer Security: The NIST Handbook” dated October 1995
- CNSSI-4009, “National Information Assurance (IA) Glossary”, dated April 2010

DEFINITIONS:

Least Privilege – The principle that security architecture be designed to grant individual users and processes only the minimum accesses to system resources and authorizations required to perform their official duties or function.

Separation of Duties – The security principle requiring the division of roles and responsibilities so that a single individual cannot subvert a critical process or function.

SUMMARY:

The implementation of least privilege is accomplished by assigning user or process access to system resources based on operational or business needs. Thus, access is granted to only those resources required to perform assigned duties. For individuals who have multiple roles within the organization requiring varying levels privileges, this assignment of access can be challenging. Often times the agency will assign a single userid to the individual and elevate the privileges for that account based on the different roles. While it may seem logical to allow the user access to all required resources using a single account, security vulnerabilities can be introduced into the system.

Associated with least privilege is separation of duties. This concept aids in maintaining the integrity of the system by preventing the abuse of elevated privileges for making unauthorized changes to the system. This objective essentially requires different individuals to perform separate functions with relation to (primarily) administrative duties. For instance, those with the ability to create and assign user access to system should not be able to access the audit logs that contain the evidence of the account actions.

USER ACCESS AND ACCOUNT MANAGEMENT:

Several factors influence the manner in which an agency implements and manages user access. Many times, the size of the agency and the technical expertise of the IT staff employed by the agency become primary drivers. Larger agencies with a broad base of technically savvy personnel normally have the ability to dedicate resources specifically to the administration and management of user access. This could translate to the use of multiple accounts for a single user performing duties requiring varying levels of access.

Smaller agencies with few or no technically experienced personnel will often assign single user accounts with the highest level of access required by users. Other smaller agencies may go as far as assigning every user an account with elevated privileges so there are no delays or problems requiring intervention by already overburdened system administrators. It is not uncommon for a smaller agency to outsource system administration duties.

Regardless of the size or resources of an organization, each agency should base the process for assigning access to system resources based on their operational requirements and a thorough risk assessment. To mitigate risk for accessing system resources, industry best security practices prescribe those individuals performing duties requiring elevated privileges be assigned a separate userid to be used in the performance of those duties. This account would be separate from a standard user account.

Why are some agencies unwilling to implement controls for least privilege? One common reason/perception is administrative overhead. There is a time factor for a system administrator to create user accounts and configure those accounts correctly based on the user's role. In larger agencies with many employees, this could add up to a significant impact on the system administrator(s) especially if there is a high level of turnover. Resources in some agencies may allow for a single system administrator dedicated strictly for account management. On the other end of the spectrum, in agencies with fewer employees, the impact may be more burdensome. While there are fewer user accounts to manage, a full-time system administrator for account management may not be feasible. Those duties then become shared between a few people or added to the duties of a lone person.

Another reason may be the burden on system administrators to remember multiple userids and passwords. This could result in the user using the same password for each account or the user writing down the credentials for ease of remembrance. Additionally, an administrator could get the credentials mixed up between accounts causing an account lockout. This could then require system administrator intervention to reset or unlock the account.

Some agencies may feel that creating additional accounts reduces system resources. Depending on the size of the agency, this could be a concern. In most cases, the number of individuals that would require a secondary account would be minimal. The impact could be limited to a slight increase in disk space usage on the systems accessed by the system administrators with the separate accounts and perhaps the server housing the account information.

THREATS:

A primary goal of attackers is to gain administrative or root privileges on a network or system. Therefore, protection of credentials with that level of access is a key to preventing unauthorized access. Attackers may use many methods in attempts to gain unauthorized, privileged access to computer or network systems. There are two common techniques that take advantage of improperly managed administrative privileges.

Phishing Attacks

In this first method, consider a small organization with limited system administrative resources. Each user is assigned an account with elevated privileges that allows them to perform a myriad of duties including gaining access to critical system security resources. Because this is the only account the user has, normal non-administrative duties are also performed with administrative rights. While checking their email, the user is fooled into reading a message and opening a malicious attachment. Because the user's account has elevated privileges, malware is now installed on the system with elevated privileges. The malware could now allow the attacker to take over the system and install other malicious software such as key loggers, sniffers, or remote control applications. Other key system resources such as firewalls, routers, switches, or intrusion detection systems are now also compromised.

Password Brute Force Guessing / Cracking

The second method may not be as easy as the first and involves the guessing or cracking of passwords on the part of the attacker. Based on human nature, we tend to develop passwords that are easy to remember and most likely contain some kind of information that is pertinent to us. Some passwords could be easily guessed with a minimal amount of social engineering or fact finding. Consider again an agency that assigns users a single account to perform all duties

including those requiring elevated privileges. A user has created a password that, while meeting the requirements of the CJIS Security Policy, is comprised of easily guessed information about the user. An attacker has previously determined the userid and is now able to begin guessing the password. Upon success, the attacker will have unauthorized access to critical system resources.

MITIGATION:

The first step to implementing least privilege is to create separate user accounts for those individuals that require elevated privileges for their duties. These duties could include system or security administration, reviewing audit logs, backup administration, or configuring network devices (e.g., firewalls, routers). The passwords associated with these accounts should have a higher level of complexity than an account without elevated privileges. By disassociating the access levels required for system administration functions from an individual's "everyday use account", should a password be compromised, access would be limited to that of a user with non-elevated privileges.

Second is to implement procedures to ensure accounts with elevated privileges are used only for those duties requiring the higher level of access. This would mean disabling or blocking access to email, web browsers, and other external facing connections. While technical processes are the preferred method of preventing the misuse of accounts with elevated privileges, written policies can be used in situations where technology does not support that type of account management.

Several governance organizations recognize the importance of the security value of Least Privilege. The Payment Card Industry (PCI) includes requirements in their Data Security Standards (DSS). The National Institute of Standards and Technology (NIST) addresses the concept of Least Privilege in its Special Publication (SP) 800-53 rev. 4. While not considered a governance organization, the System Administration, Networking, and Security (SANS) Institute publishes a list of the top 20 security controls which includes "Controlled Use of Administrator Privileges" at number 12. Although the actual security controls or required implementation may slightly differ, the concept is consistent across the groups. The actual controls from NIST and SANS are included here in this appendix.

NIST CONSIDERATIONS FOR LEAST PRIVILEGE:

NIST Special Publication 800-53 rev. 4 includes controls required for all systems under the Federal Information Security Management Act. The publication specifies the guidance for Least Privilege in the control catalog under the Access Control (AC) family and specifically as AC-6. While the NIST requirements are not enforceable under the CJIS Security Policy, they were the genesis of the Policy and do provide a sound security baseline that can be leveraged by the criminal and noncriminal justice community. AC-6 is a key control having several enhancements which, when

implemented, bolster the overall security of the information system by reducing the risk of compromise through the misuse or misconfiguration of access to system resources.

AC-6 Least Privilege

Control: The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

Supplemental Guidance: Organizations employ least privilege for specific duties and information systems. The principle of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions. Organizations consider the creation of additional processes, roles, and information system accounts as necessary, to achieve least privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational information systems. Related controls: AC-2, AC-3, AC-5, CM-6, CM-7, PL-2.

Control Enhancements:

(1) *LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS*

The organization explicitly authorizes access to [Assignment: organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information].

Supplemental Guidance: Security functions include, for example, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters. Security-relevant information includes, for example, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists. Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users. Related controls: AC-17, AC-18, AC-19.

Control Enhancements:

(2) *LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS*

The organization requires that users of information system accounts, or roles, with access to [Assignment: organization-defined security functions or security-relevant information], use non-privileged accounts or roles, when accessing nonsecurity functions.

Supplemental Guidance: This control enhancement limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies such as role-based access control and where a change of role provides the same degree of assurance in the change of access authorizations for both the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account. Related control: PL-4.

(3) *LEAST PRIVILEGE | NETWORK ACCESS TO PRIVILEGED COMMANDS*

The organization authorizes network access to [Assignment: organization-defined privileged commands] only for [Assignment: organization-defined compelling operational needs] and documents the rationale for such access in the security plan for the information system.

Supplemental Guidance: Network access is any access across a network connection in lieu of local access (i.e., user being physically present at the device). Related control: AC-17.

(4) *LEAST PRIVILEGE | SEPARATE PROCESSING DOMAINS*

The information system provides separate processing domains to enable finer-grained allocation of user privileges.

Supplemental Guidance: Providing separate processing domains for finer-grained allocation of user privileges includes, for example: (i) using virtualization techniques to allow additional privileges within a virtual machine while restricting privileges to other virtual machines or to the underlying actual machine; (ii) employing hardware and/or software domain separation mechanisms; and (iii) implementing separate physical domains. Related controls: AC-4, SC-3, SC-30, SC-32.

(5) *LEAST PRIVILEGE | PRIVILEGED ACCOUNTS*

The organization restricts privileged accounts on the information system to [Assignment: organization-defined personnel or roles].

Supplemental Guidance: Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from having access to privileged information/functions. Organizations may differentiate in the

application of this control enhancement between allowed privileges for local accounts and for domain accounts provided organizations retain the ability to control information system configurations for key security parameters and as otherwise necessary to sufficiently mitigate risk. Related control: CM-6.

(6) *LEAST PRIVILEGE | PRIVILEGED ACCESS BY NON-ORGANIZATIONAL USERS*

The organization prohibits privileged access to the information system by non-organizational users.

Supplemental Guidance:

Related control: IA-8.

(7) *LEAST PRIVILEGE | REVIEW OF USER PRIVILEGES*

The organization:

(a) Reviews [Assignment: organization-defined frequency] the privileges assigned to [Assignment: organization-defined roles or classes of users] to validate the need for such privileges; and

(b) Reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.

Supplemental Guidance: The need for certain assigned user privileges may change over time reflecting changes in organizational missions/business function, environments of operation, technologies, or threat. Periodic review of assigned user privileges is necessary to determine if the rationale for assigning such privileges remains valid. If the need cannot be revalidated, organizations take appropriate corrective actions. Related control: CA-7.

(8) *LEAST PRIVILEGE | PRIVILEGE LEVELS FOR CODE EXECUTION*

The information system prevents [Assignment: organization-defined software] from executing at higher privilege levels than users executing the software.

Supplemental Guidance: In certain situations, software applications/programs need to execute with elevated privileges to perform required functions. However, if the privileges required for execution are at a higher level than the privileges assigned to organizational users invoking such applications/programs, those users are indirectly provided with greater privileges than assigned by organizations.

(9) LEAST PRIVILEGE | AUDITING USE OF PRIVILEGED FUNCTIONS

The information system audits the execution of privileged functions.

Supplemental Guidance: Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised information system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Auditing the use of privileged functions is one way to detect such misuse, and in doing so, help mitigate the risk from insider threats and the advanced persistent threat (APT). Related control: AU-2.

(10) LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS

The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

Supplemental Guidance: Privileged functions include, for example, establishing information system accounts, performing system integrity checks, or administering cryptographic key management activities. Non-privileged users are individuals that do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users.

References: None.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD AC-6 (1) (2) (5) (9) (10)	HIGH AC-6 (1) (2) (3) (5) (9) (10)
----	-------------------------	--------------------------------------	---

SYSTEM ADMINISTRATION, NETWORKING, AND SECURITY (SANS) CONSIDERATION FOR LEAST PRIVILEGE:

There are many negative factors that affect our cyber lives: massive data loss, intellectual property theft, credit card breaches, and identity theft just to name a few. Cyber defense is rapidly evolving

to address the plethora of challenges we face. Defenders have access to a wide array of resources to combat those wishing to do harm. Ranging from the collection of vast amounts of intelligence data to security standards to training and certifications, security practitioners are well armed.

But can information overload actually worsen the problem? Organizations must decide, hopefully based on risk analysis, how to wade through all available resources and select those best suited to their own operating environment. The threats continue to evolve, the attackers become smarter, and user access more mobile. The cloud beckons and can provide reduced cost and infrastructure at a price of less control and accountability for vital information.

The SANS Institute publishes the “20 Critical Security Controls for Effective Cyber Defense”. This list of controls is the combined result of work by an international community to create, adopt, and support the controls. The components of the community provide insight, tools, information, and solutions into threats and adversaries. This list includes the control titled “Controlled Use of Administrative Privileges”. SANS describes this control as: *The process and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.*

Critical Security Control (CSC) 12: Controlled Use of Administrative Privileges

The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

ID #	Description	Category
CSC 12---1	Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.	<i>Quick win (One of the “First Five”)</i>
CSC 12---2	Use automated tools to inventory all administrative accounts and validate that each person with administrative privileges on desktops, laptops, and servers is authorized by a senior executive	<i>Quick win</i>
CSC 12---3	Configure all administrative passwords to be complex and contain letters, numbers, and special characters intermixed, and with no dictionary words present in the password. Pass phrases containing multiple dictionary words, along with special characters, are acceptable if they are of a reasonable length.	<i>Quick win</i>

CSC 12---4	Before deploying any new devices in a networked environment, change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration---level accounts.	<i>Quick win</i>
CSC 12---5	Ensure that all service accounts have long and difficult--- to--- guess passwords that are changed on a periodic basis, as is done for traditional user and administrative passwords.	<i>Quick win</i>
CSC 12---6	Passwords should be hashed or encrypted in storage. Passwords that are hashed should be salted and follow guidance provided in NIST SP 800---132 or similar guidance. Files containing these encrypted or hashed passwords required for systems to authenticate users should be readable only with super---user privileges.	<i>Quick win</i>
CSC 12---7	Utilize access control lists to ensure that administrative accounts are used only for system administration activities, and not for reading e---mail, composing documents, or surfing the Internet. Web browsers and e---mail clients especially must be configured to never run as administrator.	<i>Quick win</i>
CSC 12---8	Through policy and user awareness, require that administrators establish unique, different passwords for their administrative and non---administrative accounts. Each person requiring administrative access should be given his/her own separate account. Users should only use the Windows “administrator” or UNIX “root” accounts in emergency situations. Domain administration accounts should be used when required for system administration instead of local administrative accounts.	<i>Quick win</i>
CSC 12---9	Configure operating systems so that passwords cannot be re--- used within a timeframe of six months.	<i>Quick win</i>
CSC 12---10	Configure systems to issue a log entry and alert when an account is added to or removed from a domain administrators’ group, or when a new local administrator account is added on a system.	<i>Visibility/ Attribution</i>
CSC 12---11	Configure systems to issue a log entry and alert when unsuccessful login to an administrative account is attempted.	<i>Visibility/ Attribution</i>
CSC 12---12	Use multifactor authentication for all administrative access, including domain administrative access. Multi--- factor authentication can include a variety of techniques, to include the use of smart cards with certificates, One Time Password (OTP) tokens, and biometrics.	<i>Configuration/ Hygiene</i>

CSC 12---13 (NEW)	When using certificates to enable multi---factor certificate---based authentication, ensure that the private keys are protected using strong passwords or are stored in trusted, secure hardware tokens.	<i>Configuration/ Hygiene</i>
CSC 12---14	Block access to a machine (either remotely or locally) for administrator---level accounts. Instead, administrators should be required to access a system using a fully logged and non---administrative account. Then, once logged on to the machine without administrative privileges, the administrator should transition to administrative privileges using tools such as Sudo on Linux/UNIX, RunAs on Windows, and other similar facilities for other types of systems. Users would use their own administrative accounts and enter a password each time that is different than their user account.	<i>Configuration/ Hygiene</i>

Quick win: Implementation provides significant risk reduction without major financial, procedural, architectural, or technical changes to an environment, or that provide substantial and immediate risk reduction against very common attacks that most security-aware organizations prioritize these key controls.

Visibility / attribution: Measures to improve the process, architecture, and technical capabilities of organizations to monitor their networks and computer systems to detect attack attempts, locate points of entry, identify already-compromised machines, interrupt infiltrated attackers' activities, and gain information about the sources of an attack.

Configuration / hygiene: reduce the number and magnitude of security vulnerabilities and improve the operations of networked computer systems, with a focus on protecting against poor security practices by system administrators and end-users that could give an attacker an advantage.

SEPARATION OF DUTIES:

Separation of duties is another security control related to least privilege. Many of the same challenges faced by least privilege apply to this concept as well. Agency size and resources play a major in the implementation of separation of duties. As the name implies, some key functions should be separated between different individuals. The goal of this concept is to provide protection against a single individual's ability to circumvent system security controls to gain unauthorized access or perform unauthorized actions without colluding with other individuals.

Simply put separation of duties entails distributing certain critical mission oriented functions or system administrative support functions amongst different individuals or roles. It also includes

delineating information system support duties such as auditing, configuration control, or network security between different individuals.

As with least privilege, an agency's ability to implement separation of duties is typically based on financial and personnel resources. While a very large agency may have ready availability to those resources to ensure critical functions are spread across multiple individuals, a small agency probably does not have that luxury.

THREATS:

What effect can an individual with carte blanc access to all critical functions of a system have? Consider a single individual with the ability to install nefarious applications on a system (e.g., a keylogger). If this same individual also has the ability to edit any audit logs that would have recorded the actions of installing the software, those entries could be deleted and any evidence of the installation eliminated.

Perhaps a disgruntled system administrator wants to open a port on a firewall to allow a remote backdoor connection into the information system in order to siphon off criminal justice information. Because the perpetrator has access to the firewall and all logs, the port can be opened and the logs tampered with to eliminate records of the action.

As mentioned previously, the two concepts of least privilege and separation of duties are related. Additional threats are presented when a system administrator using a single account with unlimited elevated privileges across the information system uses that account to check email. In a successful phishing attack that compromises this account, the attacker now has unrestricted unauthorized access to all system resources and the ability to hide their tracks.

MITIGATION:

The primary method to avoid these situations is to configure system privileges and duties such that a single person is unable to effect questionable change to the system and then are able to erase any evidence of the change.

Technical configurations are most secure and sound enforceable policies compliment the technical solutions. When an information system does not support separating duties, strong policies help mitigate risk.

NIST CONSIDERATIONS FOR SEPARATION OF DUTIES:

NIST Special Publication 800-53 specifies the guidance for separation of duties in the control catalog under the Access Control (AC) family and specifically as AC-5. While the NIST requirements are not enforceable under the CJIS Security Policy, they were the genesis of the Policy and do provide a sound security baseline that can be leveraged by the criminal and noncriminal justice community. AC-5 is a relatively small control with no enhancements, but it is significant in protecting the integrity of an information system.

AC-5 Separation of Duties

Control: The organization:

- a. Separates [*Assignment: organization-defined duties of individuals*];
- b. Documents separation of duties of individuals; and
- c. Defines information system access authorizations to support separation of duties.

Supplemental Guidance: Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example: (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions. Related controls: AC-3, AC-6, PE-3, PE-4, PS-2.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD AC-5	HIGH AC-5
----	------------------	----------	-----------

G.6 Encryption

Encryption

Purpose:

This paper was created to provide assistance and guidance on encryption types, methods, and to provide general best practices in the implementation of encryption.

Attribution:

- FIPS 140 – 2, Security Requirements for Cryptographic Modules (May 2001)
- FIPS 197, Advanced Encryption Standard (Nov 2001)
- NIST SP 800-111, Guide to Storage Encryption Technologies for End User Devices
- CNSSP-15, National Information Assurance Policy on the Use of Public Standards for Secure Sharing of Information among Security Systems
- CJIS Security Policy

Definitions and Terms:

Encryption – A form of cryptology that applies a cryptographic operation to provide confidentiality of (sensitive) information.

Decryption – The inverse cryptographic operation used to convert encrypted information back into a plaintext (readable) format.

Asymmetric Encryption – A type of encryption that uses key pairs for encryption. One key is used to encrypt a message and another key to decrypt the message. Asymmetric encryption is also commonly known as public key encryption.

Symmetric Encryption – A type of encryption where the same key is used to encrypt and decrypt a message. Symmetric encryption is also known as secret key encryption.

Hybrid encryption – A type of encryption where both asymmetric encryption and symmetric encryption keys are used creating what is referred to as cipher suites. In a hybrid solution the asymmetric encryption keys are used for client/server certificate exchange to provide session integrity while the symmetric encryption keys are used for bulk data encryption to provide data confidentiality.

Authorized User/Personnel - An individual, or group of individuals, who have been appropriately vetted through a national fingerprint-based record check and have been granted access to CJI.

Summary:

CJIS Security Policy encryption requirements are intended to provide protection of the sensitive data that is criminal justice information (CJI). The primary goal of encrypting CJI is to prevent unauthorized access to this sensitive data. Encryption is a great tool that can be applied to accomplish this protection and ensure compliance with the vast majority of the CJI requirements. CJIS Security Policy Section 5.10.1.2 details when encryption is required and provides information on the exceptions to the encryption requirement.

Achieving CJIS Security Policy Compliance:

To determine when encryption is required one must first read and understand CJIS Security Policy Section 5.9.1 Physically Secure Location. The reason for this is simple: encryption is not required while within a physically secure location. Conversely, whenever CJI is transmitted or stored (at rest) outside the boundaries of a physically secure location encryption may be required. The exact standards to which the data would be required to meet are detailed along with any exceptions in CJIS Security Policy Section 5.10.1.2.

Additionally, both security awareness training and personnel security requirements can be affected by whether or not CJI is encrypted. Requirements surrounding these Policy areas is determined by answering the following question: Who has unescorted access to unencrypted CJI?

Unless personnel is escorted, security awareness training is required as correlated with the access level needed by personnel as identified in CJIS Security Policy Section 5.2. Similarly, fingerprint-based background checks as detailed in CJIS Security Policy Section 5.12 may be required on individuals to permit unescorted access to CJI.

The intent of all these requirements is to limit access to CJI to only authorized personnel. CJIS Security Policy Appendix A: Terms and Definitions defines authorized user/personnel as an individual, or group of individuals, who have been appropriately vetted through a national fingerprint-based record check and have been granted access to CJI.

What is Encryption?

Encryption is the process of encoding messages or information in such a manner that only people with the knowledge or means to decrypt the message can do so. But how does this work?

In an encryption process, legible data, referred to as plaintext, is encrypted by applying a cipher (otherwise known as an encryption algorithm or crypto key) to the data. The data then becomes encrypted and is now referred to as ciphertext. The ciphertext is essentially unreadable until decrypted. The decryption process requires the process of applying the same algorithm (crypto key) to encrypt the data in an inverse manner to convert the data back into plaintext.

Encryption is important because it allows you to securely protect data that you don't want anyone else to have access to. Encryption has been used throughout history to send “secrets” securely by some form of obfuscation to a recipient. Businesses and enterprises use encryption to protect corporate secrets and sensitive employee data, such as payroll information and personally identifiable information (PII). Governments secure classified information with encryption. Additionally, individuals may use encryption to protect personal information, such as credit card data, banking information, and passwords to guard against things like identity theft.

It should be known that encryption may not always prevent the interception of data. If the stolen data is encrypted, though, it would be extremely difficult for any of the data to be decrypted without having the decryption key. While it may be possible to decrypt the message without possessing the key, it does require large computational resources, great skill, and lots of time to accomplish such a task. Exercising encryption along with key management policies is one of the best security practices that can be put into place with regard to sensitive data security and protection.

Types of Encryption:

Symmetric Encryption

Symmetric encryption is also commonly known as secret key encryption. Symmetric encryption is a form of cryptography utilizing a singular encryption key to guise an electronic message. Its data conversion uses a mathematical algorithm along with a secret key, which results in the inability to make sense out of a message. Symmetric encryption is a two-way algorithm because the mathematical algorithm is reversed when decrypting the message along with using the same secret key.

Symmetric encryption is most often used for data protection whether at rest or in transit, especially in bulk, due to the ease and speed with which the encryption can be implemented. The most common examples of symmetric algorithms are: AES and Triple-DES (3DES or TDEA).

How it works:

To encrypt and send a message to Jane, John does the following:

1. Generates a new symmetric key
2. Encrypts the message using this new symmetric key
3. Sends the message to Jane
4. Sends the encrypted symmetric key to Jane - out of band

To decrypt this ciphertext, Jane does the following:

1. Receives the encrypted message
2. Receives the symmetric key
3. Uses the symmetric key to decrypt the message

Asymmetric Encryption

Asymmetric encryption is also commonly known as public-key encryption. Asymmetric cryptography is cryptography in which a pair of keys, a public key and a private key, are used to encrypt and decrypt a message so that it arrives securely. Initially, a network user receives a public and private key pair from a certificate authority. Any other user who wants to send an encrypted message can get the intended recipient's public key from a public directory. They use this key to encrypt the message, and they send it to the recipient. When the recipient gets the message, they decrypt it with their private key, which no one else should have access to.

Creating Key Pairs:

Asymmetric encryption requires the use of algorithms of great computational complexity to create the key pairs. This is accomplished by using a large, random number that an algorithm is applied to which generates a pair of keys for use as asymmetric key algorithms (as shown in Figure 1 below).

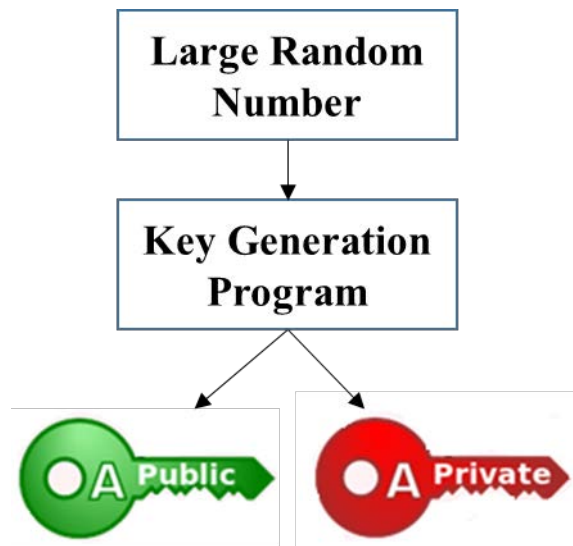


Figure 1 – Asymmetric key pair generation

Asymmetric encryption is most often used to encrypt a single message before transmission. The most common examples of asymmetric algorithms are: RSA and DSA.

How it works:

To encrypt and send a message to Jane, John does the following:

1. Obtains Jane's public key
2. Encrypts the message using Jane's public key
3. Sends the message to Jane

To decrypt this ciphertext, Jane does the following:

1. Receives the encrypted message
2. Uses her private key to decrypt the message

Advantages of Using Symmetric Encryption for Data Protection

Asymmetric encryption requires the use of algorithms with great computational complexity to create the key pairs, and therefore is not practical for large amounts of data. It is typically used for only for short messages. Also, asymmetric encryption must use a comparatively stronger key than symmetric key encryption to achieve the same level of protection as one key (public) will be published in the public directory for all to see.

Symmetric encryption is based on large, but simple algorithms which require less computation. Therefore, is much faster to create and use keys. This allows the same key to be used to encrypt and decrypt the message. So, data can be encrypted in real time. The (shared) key is sent to the recipient out of band so that it can be used to decrypt the data.

For the reasons stated above, symmetric key encryption is the preferred choice by both industry and government alike to encrypt large amounts of data (bulk encryption) simply due to the ease and real time encryption capabilities as detailed above. Additionally, a new key can be generated for every session, message transaction, etc., as desired. This means a sender won't have to use one key (public) to encrypt a message and have the recipient use another key (private) to decrypt the message.

Hybrid Encryption

Hybrid encryption solution exist where both asymmetric encryption and symmetric encryption keys are used to create what is referred to as cipher suites. In a hybrid solution the asymmetric encryption keys are used for client/server certificate exchange to provide session integrity while the symmetric encryption keys are used for bulk data encryption to provide data confidentiality.

Hybrid solutions are most often used by Internet browsers to protect data in transit. The most common examples of hybrid encryption are: TLS/SSL, PGP, IPSEC, and S/MIME.

How it works:

To encrypt a message to Jane in a hybrid cryptosystem, John does the following:

1. Obtains Jane's public key
2. Generates a new symmetric key
3. Encrypts the message using this new symmetric key
4. Encrypts the symmetric key using Jane's public key
5. Sends the message to Jane

To decrypt this hybrid cipher text, Jane does the following:

1. Receives the encrypted message
2. Receives the encrypted symmetric key
3. Uses her private key to decrypt the symmetric key
4. Uses the symmetric key to decrypt the message

Explaining Cipher Suites:

A cipher suite is a set of cryptographic algorithms used for the following:

- Protect information required to create shared keys (key exchange)
- Encrypt messages exchanged between clients and servers (bulk encryption)
- Generate message hashes and signatures to ensure the integrity of a message (message authentication)

Examples of Transport Layer Security (TLS) 1.2 Cipher Suites:

- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256

A cipher suite specifies one algorithm for each of the above tasks. For example, the TLS_RSA_WITH_AES_128_SHA256 cipher suite is used for TLS. The suite uses the RSA asymmetric algorithm for key exchange, AES with a 128-bit key for bulk data encryption, and SHA256 for message authentication.

Symmetric and Asymmetric Key Strength Comparison:

<u>Symmetric</u>		<u>Asymmetric</u>		
<u>Bits of security</u>	<u>Symmetric key algorithms</u>	<u>Finite-Field Cryptography (FFC)</u> <u>(e.g., DSA, D-H)</u> <u>Bits of security</u>	<u>Integer-Factorization Cryptography (IFC)</u> <u>(e.g., RSA)</u> <u>Bits of security</u>	<u>Elliptic-Curve Cryptography (ECC)</u> <u>(e.g., ECDSA)</u> <u>Bits of security</u>
<u>80</u>	<u>2TDEA18</u>	<u>Public key = 1024</u> <u>Private key = 160</u>	<u>Key size = 1024</u>	<u>Key size = 160-223</u>
<u>112</u>	<u>3TDEA</u>	<u>Public key = 2048</u> <u>Private key = 224</u>	<u>Key size = 2048</u>	<u>Key size = 224-255</u>
<u>128</u>	<u>AES-128</u>	<u>Public Key = 3072</u> <u>Private key = 256</u>	<u>Key size = 3072</u>	<u>Key size = 256-383</u>
<u>192</u>	<u>AES-192</u>	<u>Public key = 7680</u> <u>Private key = 384</u>	<u>Key size = 7680</u>	<u>Key size = 384-511</u>
<u>256</u>	<u>AES-256</u>	<u>Public key = 15360</u> <u>Private key = 512</u>	<u>Key size = 15360</u>	<u>Key size = 512+</u>

Figure 2 - Symmetric and asymmetric key strength comparison

As you can see in the chart provided above, the equivalent key strengths between symmetric and asymmetric key strengths do not necessarily correlate. There is a reason for this. As stated previously, asymmetric algorithms must use a comparatively stronger key than symmetric key encryption to achieve the same strength. The simplest explanation for this is because one of the keys is published to the public directory and can constantly be attacked by anyone with access to the directory. Therefore, the public key must be made of such strength that it can resist getting compromised while made public.

Federal Information Processing Standard (FIPS) 140-2 Explained

Origin of FIPS 140-2

On July 17, 1995, the National Institute of Standards and Technology (NIST) established the Cryptographic Module Validation Program (CMVP) to validate cryptographic modules to Federal Information Processing Standards (FIPS) Security Requirements for Cryptographic Modules, and other FIPS cryptography based standards. The CMVP is a joint effort between NIST and the Communications Security Establishment Canada (CSEC). FIPS 140-2, Security Requirements for Cryptographic Modules, was released on May 25, 2001 to supersede the original FIPS 140-1. Modules validated as conforming to FIPS 140-1 and FIPS 140-2 are accepted by the Federal Agencies of both countries for the protection of sensitive information.

What is FIPS 140-2?

Federal Information Processing Standard (FIPS) is a standard developed and recommended (often mandated) for use in federal-government-operated IT systems by the following two government bodies:

- The National Institute of Standards and Technology (NIST) in the United States
- The Communications Security Establishment (CSE) in Canada

FIPS 140-2 specifies the security requirements a cryptographic module must meet when utilized within a security system protecting sensitive information within information systems (computer and telecommunication systems). FIPS 140-2 specifies which encryption algorithms can be used and how encryption keys are to be generated and managed.

How does a product get certified?

Vendors of cryptographic modules can have their products tested by independent, accredited Cryptographic and Security Testing (CST) laboratories. The CST laboratories use the Derived Test

Requirements (DTR), Implementation Guidance (IG) and applicable CMVP programmatic guidance to test cryptographic modules against the applicable standards in a variety of implementations. The result of these tests are reported to NIST's Computer Security Division (CSD) and CSEC who jointly serve as the Validation Authorities for the program. These results are then reviewed and certificates would be issued if the results are determined to be acceptable.

What is the difference between being FIPS 140-2 compliant and being FIPS 140-2 certified?

It is common theme to discover a product is “FIPS compliant.” What does this mean, though? The difference between compliance and certification is not subtle. Certification requires a vast testing, verification, and validation process be performed by a CST laboratory as described in the previous section. Compliance is merely a claim stating the implementation of an encryption solution is done in accordance with the security policy related to the FIPS certification. Any claim of compliance would need to be validated and the corresponding certificate number would have to be known.

NIST has addressed related claims as shown below in their Frequently Asked Questions for the Cryptographic Module Validation Program:

A vendor makes the following claims of conformance to FIPS 140-2. Are they acceptable?

- The module has been designed for compliance to FIPS 140-2. <NO>
- Module has been pre-validated and is on the CMVP pre-validation list. <NO>
- The module will be submitted for testing. <NO>
- The module has been independently reviewed and tested to comply with FIPS 140-2. <NO>
- The module meets all the requirements of FIPS 140-2. <NO>
- The module implements FIPS Approved algorithms; including having algorithm certificates. <NO>
- The module follows the guidelines detailed in FIPS 140-2. <NO>
- The module has been validated and has received Certificate #XXXX. <YES>

A cryptographic module does not meet the requirements or conform to the FIPS 140-2 standard unless a reference can be made to the validation certificate number. The module used must also be the same version/part number as annotated on the validation certificate. Any other claims are not relevant.

To read more FAQs from NIST on FIPS certification, use the following NIST website link:
<http://csrc.nist.gov/groups/STM/cmvp/documents/CMVPFAQ.pdf>

Where can I learn more about FIPS 140-2?

For more information about the FIPS 140-2 standard, go to the following NIST website:
<http://csrc.nist.gov/cryptval/140-2.htm>

General Recommendations:

Encryption key management control is of paramount importance! Agencies should develop policies and procedures define and monitor the administrative tasks involved with protection, storage, organization, access controls and the lifecycle management of encryption keys. After all, encryption keys should not be accessible by just anyone. An encryption key management control process should ensure only authorized users have access to encryption keys. Key management is a best security practice and helps to ensure the confidentiality and integrity of CJI data and enforces key access control.

The CJIS Security Policy is a “living” document under constant review and receiving regular updates through the Advisory Policy Board (APB) process. Agencies need to always keep up to date on the latest requirements. These requirements can be found in CJIS Security Policy Section 5.10.1.2. Please contact the CJIS ISO Program anytime to address any questions or concerns about CJIS Security Policy requirements, the current APB status of CJIS Security Policy requirements, or if seeking general information or guidance.

G.7 Incident Response

Incident Response

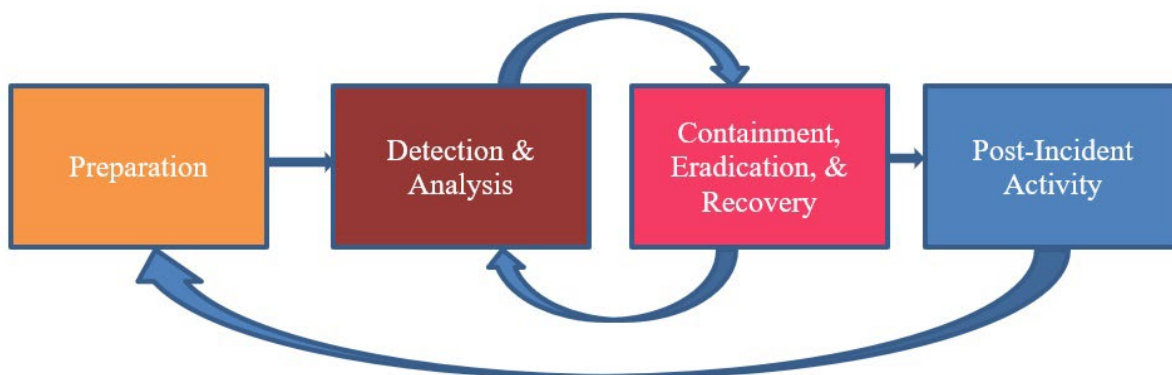
Introduction

Information technology (IT) security incident response is an important and critical component of information technology programs. Performing incident response effectively can be a complex undertaking – for that reason, establishing a successful incident response capability requires planning and resources. Everyone in an organization must be aware of IT security risks, threats, and actions to take in situations where an actual IT security incident has occurred. Even the best-secured and controlled environments can experience these security risks, threats, events, and incidents. This document provides guidelines for appropriate response to IT security incidents, and are independent of specific hardware platforms, operating systems, protocols, or applications.

The following example incidents are used to highlight appropriate actions during each phase:

- Malicious code execution
- Ransomware execution
- Denial of service attack
- Social Engineering
- Phishing

NIST Special Publication 800-61 rev. 2 outlines the “Incident Response Life Cycle” as a collection of phases – distinct sets of activities that will assist in the handling of a computer security incident, from start to finish. The following diagram explains the process flow of the incident response life cycle:



Preparation

The initial phase of the incident response life cycle, “Preparation”, involves establishing and training an incident response team, and acquiring the necessary tools and resources. A computer security incident may not have happened at this phase, but it is important to utilize all available knowledge and security measures to obtain the best posture for responding to potential future incidents. One of the most important preparation steps involves the collection, storage, and accessibility of event data and telemetry from hardware and software resources such as firewall logs, application logs, operating system logs, and other valuable sources of situational data, as well as the output of products that perform analysis on such data. Preventive measures to mitigate or eliminate future incidents are deployed during this phase, using industry best practices, data obtained from research and intelligence sources, and lessons learned from past incidents.

It is also imperative to prepare a list of contact information or notification methodologies to employ when an incident occurs, as well as notification and communication strategies within the team, with stakeholders, and with upper management and potentially other criminal justice and non-criminal justice agencies. This will help ensure that when incidents arise, the proper personnel and organizations are notified and kept informed of the circumstances regarding the incident.

Using the example incident categories outlined earlier, some overview into appropriate actions and activities for the Preparation phase can be given:

Malicious code execution

Preparation for incidents involving malicious code execution should initially involve user awareness of sources of malicious code. There are many potential sources of malicious code, such as web pages, emails, and removable media. The utilization and deployment of effective antivirus software, integrity-monitoring software, and intrusion detection and prevention software are effective measures to take to prepare for incidents involving malicious code execution.

Ransomware execution

Preparation phase activities for incidents involving ransomware execution are much the same as activities for malicious code execution, as ransomware is a specialized form of malware that encrypts potentially important or critical files, with the intention of coercing a victim to pay for a decryption key. Implementing a robust offline backup solution for these types of files is an important preparative action to take regarding the execution of ransomware. This will ensure that when ransomware attacks do happen, the mission impact is as minimal as possible and very little or no data is lost.

Denial of service attack

Denial of service attacks are given attention in the preparation phase. Defensive responses to denial of service attacks typically involve the use of a combination of attack detection

and traffic classification and response tools, aiming to block traffic identified as abusive denial of service activity. Deploying solutions such as IDS/IPS devices and software, network hardware with rate-limiting capabilities (routers, switches, and firewalls), and upstream filtering devices at the system perimeter can mitigate for denial of service attacks.

Social Engineering

Preparation for social engineering attacks starts with user awareness training. Understanding and identifying attempts to obtain information in an unauthorized manner is crucial to thwarting these types of scenarios. Social engineering is the art of manipulating people to obtain information they may not be authorized to handle. Training and routinely testing users on potential social engineering scenarios and tactics, and providing training regarding appropriate responses to requests involving personal or otherwise sensitive information (for example, passwords or criminal justice information), is an effective way to ensure social engineering attacks never traverse past the preparation phase of the incident response life cycle.

Phishing

Like social engineering, preparation for phishing attacks is imperative. Phishing is a social engineering technique attackers employ to deceive users, in a fraudulent attempt to obtain sensitive information, or to gain unauthorized access to systems. Phishing is extremely widespread, and attackers disguising fraudulent scenarios in electronic communication such as email and instant messages are the most common. User awareness of these types of tactics is paramount to prepare for phishing attacks and schemes.

Detection and Analysis

The detection and analysis phase begins when a security incident has occurred. To understand when this phase begins, there must be a capability for an intelligent determination of circumstances constituting a security incident. Specialized knowledge and highly trained personnel are necessary for this step to be effective. Many organizations employ teams of personnel who are specifically trained to handle the intricacies of the incident response life cycle. The determination of a security incident can arise from one or several circumstances simultaneously – for example:

- Trained personnel manually reviewing collected event data for evidence of compromise
- Software applications analyzing events, trends, and patterns of behavior
- The observation of suspicious or anomalous activity on a computer system

The goals of this phase are:

- To detect whether a security incident occurred
- To determine the vector (i.e., method) of attack
- To determine the impact of the incident to the mission, systems, and personnel involved in the incident

- To obtain or create intelligence products regarding attack vectors and methodologies, especially when dealing with malicious code

Prioritization of incidents is also an important decision point in the incident response life cycle, as the circumstances regarding an incident can bring the situation to a critical level. There are three major impacts to consider when addressing priority of incidents:

- **Functional Impact:** the impact to business functionality
- **Information Impact:** the impact to confidentiality, integrity, and/or availability of criminal justice information
- **Recoverability:** the amount of time and resources that must be spent on recovering from an incident

Documentation regarding an incident should be thorough and applicable to the incident. This can be crucial in incidents that may lead to legal prosecution, as well as being invaluable to efficiently document, track, handle, manage, and resolve one or more incidents at the same time.

Using the example incident categories outlined earlier, some overview into appropriate actions and activities for the Detection and Analysis phase are given:

Malicious code execution

Detection of malicious code execution is often a primary job of host-based antivirus software. Having a capable and up-to-date antivirus solution installed on a system can detect known malicious code, as well as detect potentially malicious behaviors. The delivery of malicious code to a system can be detected by network traffic analysis and protection tools and hardware. Additionally, some malicious code may produce network traffic that is indicative of successful execution, exploitation, and/or compromise of a system. Solutions such as intrusion detection/prevention systems, Security Information and Event Management (SIEM) tools, and file integrity monitoring software can provide the necessary level of fidelity to make a determination of malicious code execution.

Knowing if or when a system is infected is not always immediately evident. Security controls may have been bypassed or even disabled by the malicious code. However, systems infected by malicious code or software (i.e., malware) can exhibit several indicators. These indicators include, but are not limited to:

- Unexpected pop-up windows
- Slow start up and/or slow performance
- Suspicious hard drive activity including an unexpected lack of storage space
- Missing files
- Crashes and/or error messages
- Unexplained network activity
- Hijacked email

Analysis of malicious code can be performed in several ways. Static analysis of malicious code can be performed to determine the capabilities of the malicious code and generate actionable intelligence. Dynamic analysis of malicious code can be used to observe how the malicious code interacts with the system and what actions it performs and can often more rapidly determine the capabilities of malicious code. Both static and dynamic analysis can be performed manually, as well as in an automated fashion. Trained specialized personnel are crucial to the analysis of malicious code.

Ransomware execution

The detection of ransomware is identical to the detection of malicious code. Ransomware is specialized malicious code that encrypts potentially valuable files, generally with the intent to coerce a victim to pay a ransom for the possibility of the decryption of those files. Host-based antivirus solutions can also detect these threats, and network traffic analysis and protection tools and hardware can be used to prevent the successful execution of ransomware. SIEM tools and file integrity monitoring software can also detect the execution of ransomware.

Analysis of ransomware is identical to the analysis of malicious code, and the same intelligence can be determined in the same fashion as with the analysis of malicious code. The most obvious sign that ransomware has affected a system is the existence of encrypted files, the disappearance of certain types of files, and/or the presence of “ransom notes” on the system, which contain instructions for payment to obtain a decryption key, which may or may not be legitimate.

Denial of service attack

Denial of service (DoS) attacks are often detected at the perimeter of an organization but can also be detected within the organization as well. Often, from a user’s perspective, the signs of a DoS attack appear to be network performance or administrative maintenance related issues such as slow or broken network connections or down websites. Additionally, an administrator may notice ping time outs, event logs overflowing or alerts from network monitoring systems as issues that may identify a DoS attack. Intrusion detection and prevention software and platforms can detect denial of service attacks, as well as some network monitoring hardware and appliances, such as web application filters, routers, firewalls, and switches. Devices targeted by denial of service attacks can also detect the attacks in some instances, if they have the capabilities to determine explicit attack activity versus normal network traffic.

Analysis of denial of service attacks include the determination of the source traffic, the protocols used to generate the traffic, the service(s) targeted by the attack, and the potential impacts of the attack. Network monitoring devices can often provide these types of data, with the exception of potential impacts of denial of service attacks on systems.

Social Engineering

Detection of social engineering attacks is primarily based on the situational awareness of the individual targeted by social engineering. Given that social engineering is a broad topic that can involve the manipulation and exploitation of people in control of an information system, user awareness of social engineering attempts is crucial. If the target has security awareness training in detecting attempts to gain information or access in an unapproved manner, social engineering is easier to detect.

Analysis of social engineering attacks will generally rely on the recollection abilities of or documentation taken by the targets of the attack. Social engineering may not occur on an information system and may be completely carried out in-person. If the target can recollect or produce documentation regarding the social engineering attempt, the motivation and desired access can potentially be determined. For successful social engineering attempts, recollection and documentation of the attempt is crucial to determining the level of unauthorized access that was obtained.

Phishing

Detection of phishing attacks generally will first occur at an organization's email point of presence. Some organizations still run their own email servers, and many have migrated to cloud solutions. Having an on-premise email server or server farm or cluster will require additional functionality to detect phishing attempts. For example, the header content of the email will need to be read, as well as the content inside the body of the email, to check for potentially malicious content and potentially falsified data that may indicate a phishing email. Many cloud email providers have built this capability into their email solutions, but it is still possible for users to receive phishing emails, as attacker tactics and capabilities evolve daily. The most effective detection of phishing comes from heightened situational awareness of potential attacks. Validating the source of the email can uncover potential phishing attempts.

Analysis of phishing attacks involves examination of email headers, as well as contents of the body of the email. The body of the email may contain malicious content, attachments, or links to suspicious or malicious content. Manual or automated analysis activities can be performed on the email content. Analysis of these elements should be performed by trained specialized personnel to generate intelligence and aid with the determination of indicators of compromise.

Containment, Eradication, and Recovery

Containment activities for computer security incidents involve decision-making and the application of strategies to help control attacks and damage, cease attack activities, or reduce the impact or damage caused by the incident. Often, this requires intelligence gathered by the detection

and analysis phases of the incident – for example, identification of affected hosts, identification of attacking hosts or attackers, identification of malware and its capabilities, and identification and monitoring of attacker communication channels can be invaluable to the implementation of containment activities. In most cases, it is important to introduce containment solutions all at once, as attackers may escalate their attack activity if deployment of the strategy is delayed.

Eradication efforts for a computer security incident involve removal of latent threats from systems (such as malware on the system and user accounts that may have been created), identifying and mitigating potential vulnerabilities or misconfigurations that may have been exploited, and identification of other hosts that may have been affected within the organization.

Recovery efforts for incidents involve restoration of affected systems to normal operation. This may include actions like restoring systems from backups, rebuilding systems from an agency-approved baseline, replacing compromised files with clean versions, installing patches, changing passwords, and increasing network perimeter and host-based security.

Compromised hosts are often attacked during these phases, as attackers try to regain their foothold on compromised systems or systems on the same network or others in the logical vicinity.

Malicious code execution

Containment activities for malicious code execution involve the logical or physical isolation of the host from the attacker's control and from any mission services or systems that would be impacted by the compromised host. This may include putting the host in a restricted VLAN, using firewalls to block traffic, disconnecting it from the network completely, shutting it down, or disabling functionality. Exercise caution as malicious code may have capabilities to take further actions on a host in case communications with a command and control server are severed. It is important to understand the capabilities of the malicious code before taking containment actions.

Eradication activities include the removal of malicious code from the system. This may be as simple as removing files, configuration rules, accounts, and other persistent items that the malicious code utilizes to function and maintain a presence on the system. This phase also involves the discovery and removal of indicators of compromise on other systems, if applicable. It is imperative to remediate vulnerabilities that may have been exploited during eradication as well.

Recovery from malicious code execution generally is similar across many environments. Rebuilding the system from a clean baseline or restoring files from backup are typical activities that help restore the functionality of the system to continue the mission. Changing system passwords, installing patches, implementing tighter network access control, and

ensuring appropriate levels of logging fidelity of the information system are integral parts of the recovery process.

Ransomware execution

Containment for ransomware execution should be as swift and immediate as possible, as ransomware can execute and spread to accessible media at a rapid pace. Considering files are being encrypted or have already been encrypted, immediate action should be taken to logically or physically isolate the system by disconnecting network connectivity. It is up to the system owner whether to take the risk in powering off the system, as valuable forensic artifacts may be destroyed in the process, but it will halt the execution of the ransomware and protect potentially valuable files. Please note that containment of active ransomware execution is one of the only circumstances where measures such as immediate shutdown are recommended.

Eradication of ransomware does not need to occur in most circumstances, as the entire goal of ransomware is to encrypt files and leave “recovery” instructions to extort victims. The vast majority of ransomware will delete itself once encryption of files is complete, but it is possible that some ransomware is persistent and can remain on the system. If this is the case, analysis should be performed on the ransomware to determine its capabilities, and eradication activities will proceed in an identical fashion to malicious code execution eradication activities.

Recovery from ransomware execution involves restoring encrypted files from backup and may involve the rebuilding of an entire system depending on the extent of the encryption from the ransomware. If a robust offline backup solution for hosts is not present or not utilized on a regular basis, the loss of potentially valuable data may be incredibly costly in several areas to repair, to include man-hours, revenue, and business products, data, and intelligence.

Denial of service attack

Containment of denial of service attacks involve the modification of access control where the attack is occurring. For example, if a web or application server is experiencing a denial of service attack, the system itself, as well as network monitoring devices, should be examined to determine the source of the attack traffic. Once the source of the traffic is identified, modifications to access controls or rate-limiting features such as firewall access controls lists (ACLs) and web application filters can be employed to block the traffic. Care must be taken to determine if the observed traffic is actually intentional malicious denial of service traffic, versus heavy legitimate network traffic. Implementing access control mechanisms or rate-limiting features may negatively affect the mission of the system. It is also important to note that manual containment in this fashion may not be entirely effective, as attackers can circumvent the ACL by changing the attacking IP address, protocol, or other attribute of the connection.

Eradication is not necessarily applicable in denial of service scenarios, unless a vulnerability or misconfiguration is being exploited to cause the denial of service condition. If this is the case, take steps to remediate the vulnerability or misconfiguration.

Recovery actions depend on the available resources of the information system. For example, on-premise load balancers can be used to distribute the traffic, whether legitimate or malicious, to other less-burdened systems. Many cloud providers and content delivery networks also have denial of service mitigation capabilities. It may also be prudent to increase the resources (memory, processing capacity) of internet-facing systems so that they can handle larger amounts of traffic simultaneously.

Social Engineering

Containment regarding social engineering attacks is dependent upon the information or access that was provided to the attacker. For example, if an attacker gained access to an account on a system following a social engineering attempt, the account should be administratively disabled and all sources of event data regarding that account should be immediately collected. If sensitive data was divulged to the attacker, the impact of the exposure of that data should be examined and mitigating activity should be initiated to determine or reduce the damage of the spread of the information.

Eradication regarding social engineering attacks also depends on the information or access provided to the attacker. Removing or limiting the provided access is a pertinent eradication action. If the information provided is a credential to a system, disable and remove the credential from the system. Eradication may also involve the physical detainment or removal of personnel from a site.

Recovery actions for social engineering attacks are dependent on the information or access provided to the attacker. Additionally, security awareness training is an appropriate recovery action to ensure staff understands the threats of social engineering.

Phishing

Containment of phishing activity is tied very closely to the identification and analysis of the phishing activity. Understanding the tactics of the phishing attacker is paramount to deploying containment activities. Activities include, but are not limited to, administratively blocking sender email addresses and IPs, blocking potential malicious content in email via a web proxy, communicating with potential recipients, and implementation of email content or hyperlink blacklisting if possible. Phishing attacks can also include attempts to have users execute malicious code on systems, where containment activities regarding malicious code will be applicable.

Eradication of phishing attacks include the administrative removal of the emails from email systems, as well as eradication actions for malicious code if applicable.

Recovery from phishing attacks can include:

- Implementation and enforcement of the Domain Keys Identified Mail (DKIM) email authentication method, which can mitigate the possibility that attackers can send spoofed email
- Implementation and enforcement of Sender Policy Framework (SPF) to control and stop sender forgeries
- Implementation and enforcement of Domain-based Message Authentication, Reporting, and Conformance (DMARC), which enables message senders to indicate that their messages are protected with SPF and/or DKIM

Additionally, if malicious code is present in the phishing attack, recovery actions regarding malicious code may be applicable.

Post-Incident Activity

Post-incident activities occur after the detection, analysis, containment, eradication, and recovery from a computer security incident. Arguably one of the most important phases of incident response, post-incident activities involve the reflection, compilation, and analysis of the activities that occurred leading to the security incident, and the actions taken by those involved in the security incident, including the incident response team. Some of the important items to consider:

- Exactly what happened, and at what times?
- How well did staff and management perform in dealing with the incident?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?
- How could information sharing with other organizations have been improved?
- What corrective actions can prevent similar actions in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

Smaller incidents, and those that are similar to others that have been well documented, do not necessarily need much focus in this phase of incident response. Larger and less-understood security incidents should be the focus of a comprehensive post-mortem evaluation that outlines

many of the items listed above and should include personnel that can have a direct impact on or are directly affected or responsible for the involved systems.

Post-incident activities such as these also help to serve as training opportunities for all parties involved in the incident, from victims, to system administration personnel, to incident responders.

Malicious code execution

Post-incident activities for malicious code execution generally will follow similar patterns. A timeline of activity should have been prepared using digital forensic data collected during the detection and analysis phases of the incident. This timeline should include all affected systems and times of all activities and actions taken during the incident. Steps that victims and system administrators may have taken during the course of the incident, as well as in close proximity to the time range of the incident, are valuable items to document and discuss. Any deviation from organizational policy should be noted and taken as training items or assigned consequences in accordance with organizational policies. It may also be pertinent to ensure that appropriate information and intelligence sharing was performed during and after the incident occurred. Corrective actions that may have prevented the execution of malicious code, such as antivirus solutions, restrictions on where executables can run, tightened permissions, and script blockers for browsers, should be considered as a mitigation for the risks posed by malicious code threats. Web proxy blocks from information discovered during analysis can be utilized to ensure that malicious hosts are not contacted.

Ransomware execution

Post-incident activities for ransomware execution include all the activities involved with malicious code execution, with the addition of ensuring the functionality of a robust offline backup solution. An offline backup solution ensures that backup data is kept inaccessible to ransomware threats and is available if ransomware is successfully executed. A functional and frequent (such as daily incremental and weekly full) backup process helps ensure that business continuity is maintained in the event of issues and incidents.

Denial of service attack

Denial of service post-incident activities should include a timeline of traffic activities, as well as organizational responses to the attack traffic as well as the timeline of any business impacts and the damage associated with the impacts. Any attack precursors should be investigated and noted, and intelligence implemented to notify personnel and potentially take action as soon as attack traffic is observed. Impacts on affected systems should be noted, and a consensus should be reached on whether the systems should be upgraded or supplemented with load-balancing capabilities.

Social Engineering

Post-incident activities for social engineering incidents should include a timeline that includes all applicable activities, such as points of contact, narratives from the parties involved, CCTV footage (if applicable), system and network log files, and physical access control logging data. If unauthorized access was obtained, the impact of the access should be assessed and mitigating factors should be identified for inclusion to reduce the risk of future incidents (such as multifactor authentication, physical locks, greater CCTV coverage, improved physical access control, etc.). Security awareness training should be imperative if policy was breached, and information or access was given to unauthorized parties.

Phishing

Phishing post-incident activities should also include a timeline of actions taken since the phishing email was received, to include descriptions of the type of phishing campaign observed (malicious code, financial exploitation, credential harvesting, etc.), malicious attachments contained (if any), malicious or suspicious links in the body of emails, as well as narratives from recipients of the email and any potential victims, either self-reported or discovered through email, network, or host-based monitoring. If malicious code was included in the campaign, typical post-incident activities involving malicious code should be considered as well. Training opportunities can often arise from phishing attacks, whether successful or not, that can be valuable in giving employees better situational awareness regarding phishing.

The CJIS Security Policy requires each agency with access to CJI to establish operational incident handling procedures (i.e., a local policy). Gleaning from the requirements in Section 5.3 Incident Response, the local policy may include the following elements:

- Overall incident handling procedures. This section describes and identifies the processes used locally how the agency successfully prepares for, manages, and recovers from an incident. It includes sections on:
 - Preparation
 - Detection and Analysis
 - Containment
 - Recovery
 - User response activities
- How the agency performs incident reporting. This section describes the process of notifying internal and external partners when an incident has occurred and how the incident is documented. It includes sections on:
 - Internal and external points of contact
 - Required tracking and reporting documents
 - Escalation procedures
- Incident management procedures. This section describes the agency's approach to a consistent and repeatable approach to managing incidents. It includes sections on:
 - Roles and responsibilities

- Incident-related information collection
- Updating policies with lessons learned
- Collection of evidence
- Incident response training
- Document and artifact retention

G.8 Secure Coding

Secure Coding

This appendix documents a source of information on best practices and standards for secure coding. With the increased use of software products and the rapid pace of modern software development, it is essential to discover and resolve insecure software risks. The mitigations and guidelines to reduce these common risks can be found in secure coding best practices.

Understanding how software applications work can be a daunting thing; however, it could be key to know if data security is in jeopardy. Awareness of secure coding practices allows an agency to review potential vendors and their products prior to purchase and implementation. It also empowers the agency with the knowledge of the questions to ask a vendor of how the software was developed and whether the vendor uses secure coding practices or standards.

Additionally, the information in this appendix can provide a path forward for agencies with the internal capability to produce “in-house” software applications. By implementing security during the code writing process, security is “baked in” and there is more trust the software will aid in protecting the information it processes.

Open Web Application Security Project (OWASP) Foundation

The OWASP Foundation is a not-for-profit charitable organization focused on improving the security of software. OWASP operates as a community of like-minded professionals to provide unbiased and practical information about application security (AppSec) through software tools and documentation. These materials are available under a free and open software license, which can be located at the link below.

https://www.owasp.org/index.php/Main_Page

Software is becoming increasingly complex and connected, and the difficulty of achieving application security increases exponentially. The rapid pace of modern software development processes makes the most common risks essential to discover and resolve quickly and accurately.

The OWASP Foundation publishes the Top 10 Application Security Risks, which focus on the most serious web application security risks. The OWASP Top 10 is based primarily on 40 plus data submissions from firms that specialize in application security and an industry survey that was completed by over 500 individuals. This data spans vulnerabilities gathered from hundreds of organizations and over 100,000 real world applications and application program interfaces (API). The Top 10 items are selected and prioritized according to this data, in combination with consensus estimates of exploitability, detectability, and impact.

A primary aim of the OWASP Top 10 is to educate developers, designers, architects, managers, and organizations about the consequences of the most common and most important web application security weaknesses. The Top 10 provides basic techniques to protect against these high risks problem areas, and provides guidance on a path forward.

The OWASP Top 10 focuses on identifying the most serious web application security risks for a broad array of organizations. For each of these risks, generic information about likelihood and technical impact using the following simple ratings scheme, which is based on the OWASP Risk Rating Methodology.

Figure G.8-A

T10

OWASP Top 10
Application Security Risks – 2017

6

A1:2017-Injection

Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

A2:2017-Broken Authentication

Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.

A3:2017-Sensitive Data Exposure

Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.

A4:2017-XML External Entities (XXE)

Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.

A5:2017-Broken Access Control

Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.

A6:2017-Security Misconfiguration

Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched and upgraded in a timely fashion.

A7:2017-Cross-Site Scripting (XSS)

XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

A8:2017-Insecure Deserialization

Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.

A9:2017-Using Components with Known Vulnerabilities

Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.

A10:2017-Insufficient Logging & Monitoring

Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

Each organization is unique, and so are the threat actors for that organization, their goals, and the impact of any breach. It is critical to understand the risk to your organization based on applicable threat agents and business impacts.

Application Security Risks

The figures immediately below illustrate the path of a sample threat beginning with the threat agent and ending with the target or affected business resource. Various paths are available but the agent would normally select the path of least resistance which would be the most vulnerable and with the fewest number of effective security controls.

The sample risk matrix can be used to assign in the various aspects of potential vulnerability. Each column corresponds to a phase in the attack process. In the matrix, a lower value represents less risk and is more desirable.

Concerning secure coding practices, when security is built-in during code development, vulnerabilities can be identified and controls included reducing the overall risk to information processed by the code.

Figure G.8-B Sample Threat Path

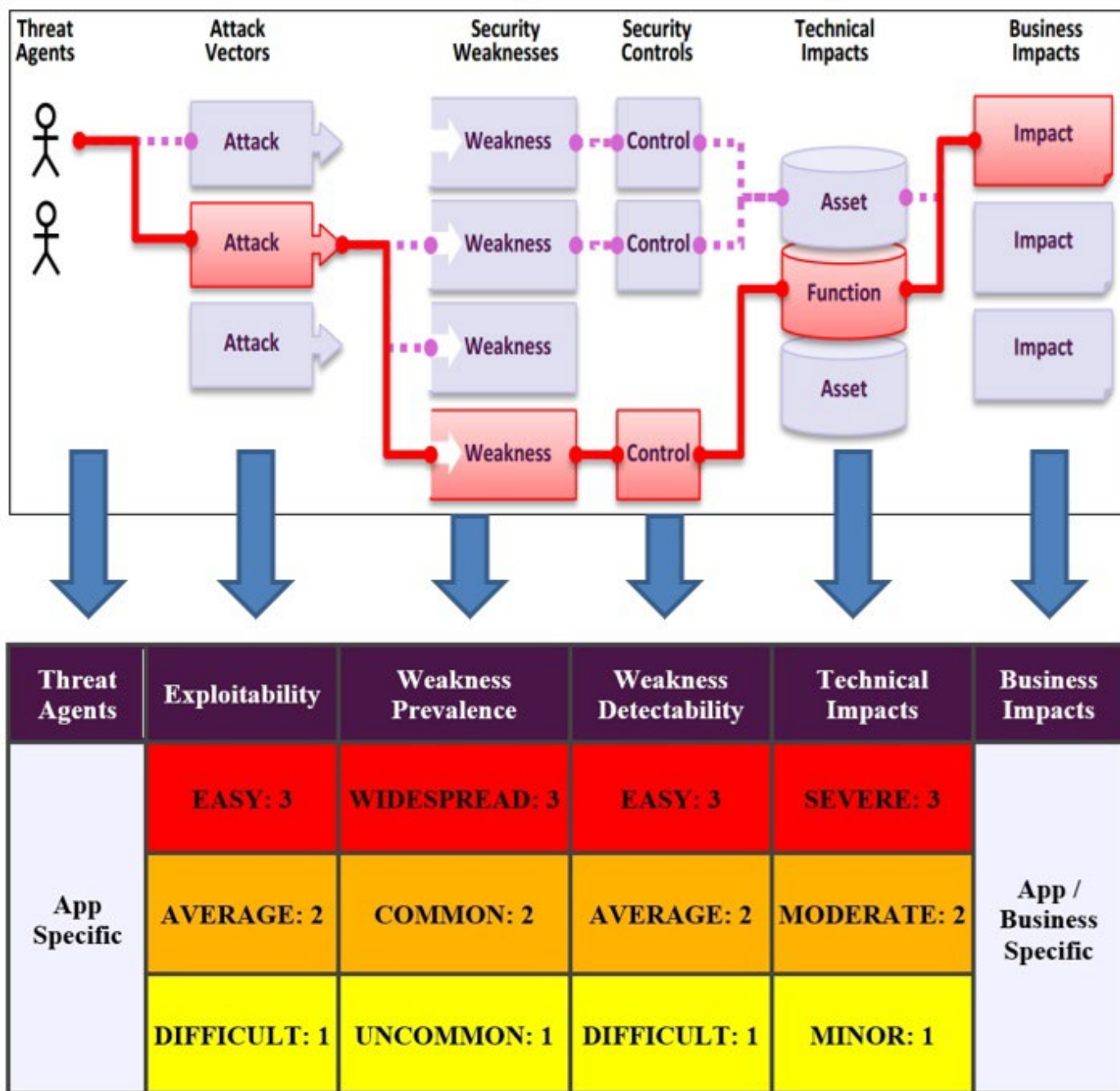


Figure G.8-C General Risk Matrix

To understand these risks for a particular application or organization, you must consider your own specific threat agents and business impacts. Even severe software weaknesses may not present a serious risk if there are no threat agents in a position to perform the necessary attack or the business impact is negligible for the assets involved. The following table presents a summary of the 2017 Top 10 Application Security Risks, and the risk factors that have been assigned to each risk.

Figure G.8-D Top 10 Risk Factor Summary

RISK							Score
	Threat Agents	Exploitability	Prevalence	Detectability	Technical	Business	
A1:2017-Injection	App Specific	EASY: 3	COMMON: 2	EASY: 3	SEVERE: 3	App Specific	8.0
A2:2017-Authentication	App Specific	EASY: 3	COMMON: 2	AVERAGE: 2	SEVERE: 3	App Specific	7.0
A3:2017-Sens. Data Exposure	App Specific	AVERAGE: 2	WIDESPREAD: 3	AVERAGE: 2	SEVERE: 3	App Specific	7.0
A4:2017-XML External Entities (XXE)	App Specific	AVERAGE: 2	COMMON: 2	EASY: 3	SEVERE: 3	App Specific	7.0
A5:2017-Broken Access Control	App Specific	AVERAGE: 2	COMMON: 2	AVERAGE: 2	SEVERE: 3	App Specific	6.0
A6:2017-Security Misconfiguration	App Specific	EASY: 3	WIDESPREAD: 3	EASY: 3	MODERATE: 2	App Specific	6.0
A7:2017-Cross-Site Scripting (XSS)	App Specific	EASY: 3	WIDESPREAD: 3	EASY: 3	MODERATE: 2	App Specific	6.0
A8:2017-Insecure Deserialization	App Specific	DIFFICULT: 1	COMMON: 2	AVERAGE: 2	SEVERE: 3	App Specific	5.0
A9:2017-Vulnerable Components	App Specific	AVERAGE: 2	WIDESPREAD: 3	AVERAGE: 2	MODERATE: 2	App Specific	4.7
A10:2017-Insufficient Logging&Monitoring	App Specific	AVERAGE: 2	WIDESPREAD: 3	DIFFICULT: 1	MODERATE: 2	App Specific	4.0

Whether you are new to web application security or already very familiar with these risks, the task of producing a secure web application or fixing an existing one can be difficult. If you have to manage a large application portfolio, this task can be daunting.

To help organizations, developers, testers and managers reduce their application security risks in a cost-effective manner; OWASP has produced numerous free and open resources that you can use to address application security in your organization. The following are some of the many resources OWASP has produced to help organizations produce secure web applications and APIs.

Get Started:

- Document all applications and associated data assets.
- Larger organizations should consider implementing a Configuration Management Database (CMDB).
- Establish an application security program to conduct analysis to define key improvement areas and an execution plan.

Risk Based Portfolio Approach:

- Identify the protection needs of your application portfolio from a business perspective.
- Establish a common risk-rating model with a consistent set of likelihood and impact factors reflective of your organization's tolerance for risk.
- Measure and prioritize all applications and APIs and add results to CMDB.

Enable with a Strong Foundation:

- Establish a set of policies and standards that provide an application security baseline for all development teams to adhere to.
- Define a common set of reusable security controls that complement these policies and standards and provide design and development guidance on their use.

Integrate Security into Existing Processes:

- Define and integrate secure implementation and verification activities into existing development and operational processes.
 - Activities include threat modeling, secure design and design review, secure coding and code review, penetration testing, and remediation.

Application Security Requirements - to produce a secure web application, you must define what secure means for that application.

- [Application Security Verification Standard \(ASVS\):](https://www.owasp.org/index.php/ASVS)
<https://www.owasp.org/index.php/ASVS>
- [OWASP Secure Software Contract Annex:](https://www.owasp.org/index.php/OWASP_Secure_Software_Contract_Annex)
https://www.owasp.org/index.php/OWASP_Secure_Software_Contract_Annex

Application Security Architecture - retrofitting security into your applications and APIs, it is far more cost effective to design the security in from the start.

- OWASP Prevention Cheat Sheets:

https://www.owasp.org/index.php/OWASP_Cheat_Sheet_Series

Standard Security Controls - building strong and usable security controls is difficult. Using a set of standard security controls radically simplifies the development of secure applications and APIs.

- OWASP Proactive Controls:
https://www.owasp.org/index.php/OWASP_Proactive_Controls

Secure Development Lifecycle - to improve the process your organization follows when building applications and APIs, organizations formulate and implement a strategy for software security that is tailored to the specific risks facing their organization.

- OWASP Software Assurance Maturity Model (SAMM):
https://www.owasp.org/index.php/OWASP_SAMM_Project
- OWASP Application Security Guide for CISOs:
https://www.owasp.org/index.php/Application_Security_Guide_For_CISOs

Application Security Education – hands-on learning about vulnerabilities to help educate developers on web application security.

- OWASP Education Project:
https://www.owasp.org/index.php/Category:OWASP_Education_Project
- OWASP WebGoat:
<https://www.owasp.org/index.php/WebGoat>
- OWASP Broken Web Application Project:
https://www.owasp.org/index.php/OWASP_Broken_Web_Applications_Project

Understand the Threat Model – be sure to understand the priorities when it comes to threat model.

- OWASP Testing Guide:
https://www.owasp.org/index.php/OWASP_Testing_Project
- [Application Security Verification Standard \(ASVS\):](https://www.owasp.org/index.php/ASVS)
<https://www.owasp.org/index.php/ASVS>

Testing Strategies – choose the simplest, fastest, most accurate technique to verify each requirement.

- OWASP Security Knowledge Framework:
https://www.owasp.org/index.php/OWASP_Security_Knowledge_Framework

- [Application Security Verification Standard \(ASVS\):
https://www.owasp.org/index.php/ASVS](https://www.owasp.org/index.php/ASVS)

APPENDIX H: SECURITY ADDENDUM

The following pages contain:

The legal authority, purpose, and genesis of the Criminal Justice Information Services Security Addendum (H-2-H-4);

An example of a contract addendum (H-5);

The Security Addendum itself (H-6-H-7);

The Security Addendum Certification page (H-8).

**FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM**

**Legal Authority for and Purpose and Genesis of the
Security Addendum**

Traditionally, law enforcement and other criminal justice agencies have been responsible for the confidentiality of their information. Accordingly, until mid-1999, the Code of Federal Regulations Title 28, Part 20, subpart C, and the National Crime Information Center (NCIC) policy paper approved December 6, 1982, required that the management and exchange of criminal justice information be performed by a criminal justice agency or, in certain circumstances, by a noncriminal justice agency under the management control of a criminal justice agency.

In light of the increasing desire of governmental agencies to contract with private entities to perform administration of criminal justice functions, the FBI sought and obtained approval from the United States Department of Justice (DOJ) to permit such privatization of traditional law enforcement functions under certain controlled circumstances. In the Federal Register of May 10, 1999, the FBI published a Notice of Proposed Rulemaking, announcing as follows:

1. Access to CHRI [Criminal History Record Information] and Related Information, Subject to Appropriate Controls, by a Private Contractor Pursuant to a Specific Agreement with an Authorized Governmental Agency To Perform an Administration of Criminal Justice Function (Privatization). Section 534 of title 28 of the United States Code authorizes the Attorney General to exchange identification, criminal identification, crime, and other records for the official use of authorized officials of the federal government, the states, cities, and penal and other institutions. This statute also provides, however, that such exchanges are subject to cancellation if dissemination is made outside the receiving departments or related agencies. Agencies authorized access to CHRI traditionally have been hesitant to disclose that information, even in furtherance of authorized criminal justice functions, to anyone other than actual agency employees lest such disclosure be viewed as unauthorized. In recent years, however, governmental agencies seeking greater efficiency and economy have become increasingly interested in obtaining support services for the administration of criminal justice from the private sector. With the concurrence of the FBI's Criminal Justice Information Services (CJIS) Advisory Policy Board, the DOJ has concluded that disclosures to private persons and entities providing support services for criminal justice agencies may, when subject to appropriate controls, properly be viewed as permissible disclosures for purposes of compliance with 28 U.S.C. 534.

We are therefore proposing to revise 28 CFR 20.33(a)(7) to provide express authority for such arrangements. The proposed authority is similar to the authority that already exists in 28 CFR 20.21(b)(3) for state and local CHRI systems. Provision of CHRI under this authority would only be permitted pursuant to a specific agreement with an authorized governmental agency for the purpose of providing services for the administration of criminal justice. The agreement would be required to incorporate a security addendum approved by the Director of the FBI (acting for the Attorney General). The security

addendum would specifically authorize access to CHRI, limit the use of the information to the specific purposes for which it is being provided, ensure the security and confidentiality of the information consistent with applicable laws and regulations, provide for sanctions, and contain such other provisions as the Director of the FBI (acting for the Attorney General) may require. The security addendum, buttressed by ongoing audit programs of both the FBI and the sponsoring governmental agency, will provide an appropriate balance between the benefits of privatization, protection of individual privacy interests, and preservation of the security of the FBI's CHRI systems.

The FBI will develop a security addendum to be made available to interested governmental agencies. We anticipate that the security addendum will include physical and personnel security constraints historically required by NCIC security practices and other programmatic requirements, together with personal integrity and electronic security provisions comparable to those in NCIC User Agreements between the FBI and criminal justice agencies, and in existing Management Control Agreements between criminal justice agencies and noncriminal justice governmental entities. The security addendum will make clear that access to CHRI will be limited to those officers and employees of the private contractor or its subcontractor who require the information to properly perform services for the sponsoring governmental agency, and that the service provider may not access, modify, use, or disseminate such information for inconsistent or unauthorized purposes.

Consistent with such intent, Title 28 of the Code of Federal Regulations (C.F.R.) was amended to read:

§ 20.33 Dissemination of criminal history record information.

- a) Criminal history record information contained in the Interstate Identification Index (III) System and the Fingerprint Identification Records System (FIRS) may be made available:
 - 1) To criminal justice agencies for criminal justice purposes, which purposes include the screening of employees or applicants for employment hired by criminal justice agencies.
 - 2) To noncriminal justice governmental agencies performing criminal justice dispatching functions or data processing/information services for criminal justice agencies; and
 - 3) To private contractors pursuant to a specific agreement with an agency identified in paragraphs (a)(1) or (a)(6) of this section and for the purpose of providing services for the administration of criminal justice pursuant to that agreement. The agreement must incorporate a security addendum approved by the Attorney General of the United States, which shall specifically authorize access to criminal history record information, limit the use of the information to the purposes for which it is provided, ensure the security and confidentiality of the information consistent with these regulations, provide for sanctions, and contain such other provisions as the Attorney General may require. The power

and authority of the Attorney General hereunder shall be exercised by the FBI Director (or the Director's designee).

This Security Addendum, appended to and incorporated by reference in a government-private sector contract entered into for such purpose, is intended to insure that the benefits of privatization are not attained with any accompanying degradation in the security of the national system of criminal records accessed by the contracting private party. This Security Addendum addresses both concerns for personal integrity and electronic security which have been addressed in previously executed user agreements and management control agreements.

A government agency may privatize functions traditionally performed by criminal justice agencies (or noncriminal justice agencies acting under a management control agreement), subject to the terms of this Security Addendum. If privatized, access by a private contractor's personnel to NCIC data and other CJIS information is restricted to only that necessary to perform the privatized tasks consistent with the government agency's function and the focus of the contract. If privatized the contractor may not access, modify, use or disseminate such data in any manner not expressly authorized by the government agency in consultation with the FBI.

EXAMPLE OF A CONTRACT ADDENDUM

AMENDMENT NO. ____ TO THE CONTRACT BETWEEN
[PARTY NO. 1] AND [PARTY NO. 2], ENTERED INTO [DATE]

[Name of Law Enforcement Agency] and [Party No. 2], upon notification and pursuant to Paragraph/Section No. ____ [the amendment clause of the original contract] of that certain contract entered into by these parties on [date][and entitled “____”], hereby amend and revise the contract to include the following:

1. Access to and use of criminal history record information and other sensitive information maintained in [state and] FBI-managed criminal justice information systems by [private party] are subject to the following restrictions:

- a.
- b.
- c.

and

- d. The Security Addendum appended hereto, which is incorporated by reference and made a part thereof as if fully appearing herein.

This amendment is effective the ____ day of _____, 20__.

On behalf of [Party No. 1]:

_____ Printed Name	_____ Title
_____ Signature	_____ Date

On behalf of [Party No. 2]:

_____ Printed Name	_____ Title
_____ Signature	_____ Date

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A-130 as “security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.”

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI’s information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

1.00 Definitions

1.01 Contracting Government Agency (CGA) – the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

1.02 Contractor – a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

2.00 Responsibilities of the Contracting Government Agency.

2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed by hand or via digital signature (see glossary for definition of digital signature).

3.00 Responsibilities of the Contractor.

3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed and all subsequent versions), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

4.00 Security Violations.

4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

4.02 Security violations can justify termination of the appended agreement.

4.03 Upon notification, the FBI reserves the right to:

- a. Investigate or decline to investigate any report of unauthorized use;
- b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CGA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

5.00 Audit

5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

6.00 Scope and Authority

6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.04 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.05 All notices and correspondence shall be forwarded by First Class mail to:

Information Security Officer

Criminal Justice Information Services Division, FBI

1000 Custer Hollow Road

Clarksburg, West Virginia 26306

**FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM**

CERTIFICATION

I hereby certify that I am familiar with the contents of (1) the Security Addendum, including its legal authority and purpose; (2) the NCIC Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

Printed Name/Signature of Contractor Employee

Date

Printed Name/Signature of Contractor Representative

Date

Organization and Title of Contractor Representative

APPENDIX I: REFERENCES

White House Memo entitled “Designation and Sharing of Controlled Unclassified Information (CUI)”, May 9, 2008

[CJIS RA] *CJIS Security Policy Risk Assessment Report*; August 2008; For Official Use Only; Prepared by: Noblis; Prepared for: U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division, 1000 Custer Hollow Road, Clarksburg, WV 26306

[CNSS Instruction No. 4009] *National Information Assurance (IA) Glossary*; Committee on National Security Systems (CNSS) Instruction No. 4009; 26 April 2010

[FBI SA 8/2006] *Federal Bureau of Investigation, Criminal Justice Information Services, Security Addendum*; 8/2006; Assistant Director, Criminal Justice Information Services, FBI, 1000 Custer Hollow Road, Clarksburg, West Virginia 26306

[FISMA] *Federal Information Security Management Act of 2002*; House of Representatives Bill 2458, Title III–Information Security

[FIPS 199] *Standards for Security Categorization of Federal Information and Information Systems*; Federal Information Processing Standards Publication, FIPS PUB 199; February 2004

[FIPS 200] *Minimum Security Requirements for Federal Information and Information Systems*; Federal Information Processing Standards Publication, FIPS PUB 200; March 2006

[FIPS 201] *Personal Identity Verification for Federal Employees and Contractors*; Federal Information Processing Standards Publication, FIPS PUB 201-1

[NIST SP 800–14] *Generally Accepted Principles and Practices for Securing Information Technology Systems*; NIST Special Publication 800–14

[NIST SP 800–25] *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*; NIST Special Publication 800–25

[NIST SP 800–30] *Risk Management Guide for Information Technology Systems*; NIST Special Publication 800–36

[NIST SP 800–32] *Introduction to Public Key Technology and the Federal PKI Infrastructure*; NIST Special Publication 800–32

[NIST SP 800–34] *Contingency Planning Guide for Information Technology Systems*; NIST Special Publication 800–34

[NIST SP 800–35] *Guide to Information Technology Security Services*; NIST Special Publication 800–35

[NIST SP 800–36] *Guide to Selecting Information Technology Security Products*; NIST Special Publication 800–36

[NIST SP 800–39] *Managing Risk from Information Systems, An Organizational Perspective*; NIST Special Publication 800–39

- [NIST SP 800–40] *Procedures for Handling Security Patches*; NIST Special Publication 800–40
- [NIST SP 800–44] *Guidelines on Securing Public Web Servers*; NIST Special Publication 800–44
- [NIST SP 800–45] *Guidelines on Electronic Mail Security*; NIST Special Publication 800–45, Version 2
- [NIST SP 800–46] *Security for Telecommuting and Broadband Communications*; NIST Special Publication 800–46
- [NIST SP 800–48] *Wireless Network Security: 802.11, Bluetooth, and Handheld Devices*; NIST Special Publication 800–48
- [NIST SP 800–52] *Guidelines on the Selection and Use of Transport Layer Security*; NIST Special Publication 800–52
- [NIST SP 800–53] *Recommended Security Controls for Federal Information Systems*; NIST Special Publication 800–53, Revision 2
- [NIST SP 800–53A] *Guide for Assessing the Security Controls in Federal Information Systems, Building Effective Security Assessment Plans*; NIST Special Publication 800–53A
- [NIST SP 800–58] *Security Considerations for Voice over IP Systems*; NIST Special Publication 800–58
- [NIST SP 800–60] *Guide for Mapping Types of Information and Information Systems to Security Categories*; NIST Special Publication 800–60, Revision 1, DRAFT
- [NIST SP 800–63–1] *Electronic Authentication Guideline*; NIST Special Publication 800–63–1; DRAFT
- [NIST SP 800–64] NIST Special Publication 800–64
- [NIST SP 800–66] *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA)*; NIST Special Publication 800–66
- [NIST SP 800–68] *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist*; NIST Special Publication 800–68
- [NIST SP 800–70] *Security Configuration Checklists Program for IT Products*; NIST Special Publication 800–70
- [NIST SP 800–72] *Guidelines on PDA Forensics*; NIST Special Publication 800–72
- [NIST SP 800–73] *Integrated Circuit Card for Personal Identification Verification*; NIST Special Publication 800–73; Revision 1
- [NIST SP 800–76] *Biometric Data Specification for Personal Identity Verification*; NIST Special Publication 800–76
- [NIST SP 800–77] *Guide to IPsec VPNs*; NIST Special Publication 800–77
- [NIST SP 800–78] *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*; NIST Special Publication 800–78
- [NIST SP 800–81] *Secure Domain Name System (DNS) Deployment Guide*; NIST Special Publication 800–81

- [NIST SP 800–84] *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*; NIST Special Publication 800–84
- [NIST SP 800–86] *Guide to Integrating Forensic Techniques into Incident Response*; NIST Special Publication 800–86
- [NIST SP 800–87] *Codes for the Identification of Federal and Federally Assisted Agencies*; NIST Special Publication 800–87
- [NIST SP 800–96] *PIV Card / Reader Interoperability Guidelines*; NIST Special Publication 800–96
- [NIST SP 800–97] *Guide to IEEE 802.11i: Robust Security Networks*; NIST Special Publication 800–97
- [NIST SP 800–121] *Guide to Bluetooth Security*; NIST Special Publication 800–121
- [NIST SP 800–124] *Guidelines on Cell Phone and PDA Security*; NIST Special Publication 800–124
- [NIST SP 800–125] *Guide to Security for Full Virtualization Technologies*; NIST Special Publication 800–125
- [NIST SP 800–144] *Guidelines on Security and Privacy in Public Cloud Computing*; NIST Special Publication 800–144
- [NIST SP 800–145] *The NIST Definition of Cloud Computing*; NIST Special Publication 800–145
- [NIST SP 800–146] *Cloud Computing Synopsis and Recommendations*; NIST Special Publication 800–146
- [OMB A–130] *Management of Federal Information Resources*; Circular No. A–130; Revised; February 8, 1996
- [OMB M–04–04] *E-Authentication Guidance for Federal Agencies*; OMB Memo 04–04; December 16, 2003
- [OMB M–06–15] *Safeguarding Personally Identifiable Information*; OMB Memo 06–15; May 22, 2006
- [OMB M–06–16] *Protection of Sensitive Agency Information*; OMB Memo 06–16; June 23, 2006
- [OMB M–06–19] *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*; OMB Memo 06–19; July 12, 2006
- [OMB M–07–16] *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*; OMB Memo 07–16; May 22, 2007
- [Surviving Security] *Surviving Security: How to Integrate People, Process, and Technology*; Second Edition; 2004
- [USC Title 5, Section 552] *Public information; agency rules, opinions, orders, records, and proceedings*; United States Code, Title 5 – Government Agency and Employees, Part I – The Agencies Generally, Chapter 5 – Administrative Procedure,

Subchapter II – Administrative Procedure, Section 552. Public information;
agency rules, opinions, orders, records, and proceedings

[USC Title 44, Section 3506] *Federal Information Policy*; 01/02/2006; United States Code, Title
44 – Public Printing and Documents; Chapter 35 – Coordination of Federal Information Policy;
Subchapter I – Federal Information Policy, Section 3506



Requirements Companion Document to the FBI CJIS Security Policy Version 6.0

12/27/2024



Prepared by:
CJIS Information Security Officer

Recommended changes to version 5.9.5 of the *CJIS Security Policy (CSJISECPOL)* were approved by the Advisory Policy Board (APB) in June 2024 and subsequently approved by the Director, FBI. The Policy contains current requirements carried over from previous versions along with newly approved requirements for agencies to implement.

The “Summary of Changes” page lists the sections with changes.

Based on the “*CJISSECPOL* Security Control Priority and Implementation Deadlines” topic paper endorsed by the Fall 2023 APB and approved by the FBI Director, changes have been made to the “Audit / Sanction Date” column and a new “Priority” column has been added. The “Audit / Sanction Date” column indicates the date when modernized security controls will become sanctionable for audit. Requirements and modernized controls existing in *CJISSECPOL* version 5.9 are indicated in **GREEN** and state ‘Existing’. New requirements modernized after that version are not yet sanctionable, indicated in **YELLOW**, and state “Zero-cycle”. **The “Zero-cycle” begins for all agencies on October 1, 2024.** The “Priority” column indicates the approved assigned priority for each control. Priority 1 [P1] controls are immediately sanctionable upon publication of *CJISSECPOL* they first appear in. They are marked with date of publication of the version of the *CJISECPOL* they first appear in.

The document also contains the “cloud matrix” consisting of additional columns describing who (CJIS*/CSO, Agency, Cloud Service Provider or both the agency and service provider) has the technical capability to perform the actions necessary to ensure a particular requirement is being met. **NOTE: The Agency is always ultimately accountable to ensure Policy compliance.** Three sub-columns are labeled IaaS, PaaS and SaaS and depict the type of cloud services being leveraged by the Agency from the Cloud Service Provider. Respectively, these cloud service models are:

- IaaS – Infrastructure as a Service
- PaaS – Platform as a Service
- SaaS – Software as a Service

Responsibility is color-coded within the columns based on the agreed ability to perform the actions necessary to meet requirements. They are as follows:

Dark Gray	CJIS*/CSO
Dark Green	Agency
Dark Blue	Service Provider
Orange	Both
Aqua	TBD

Some modernized controls have not been assigned cloud matrix values and those corresponding cells are colored in Aqua and contain TBD.

* - CJIS means the FBI CJIS Division.

Please refer questions or comments about this document or the current version of the *CJISSECPOL* to your respective State CJIS Information Security Officer, CJIS Systems Officer, Compact Officer, or the FBI CJIS ISO at iso@fbi.gov.

SUMMARY OF CHANGES

Version 6.0

APB Approved Changes

1. **Modernizing the Executive Summary, Section 1: Introduction, Section 2: *CJISSECPOL* Approach, and Section 3: Roles and Responsibilities in the *CJISSECPOL*, Spring 2024, APB#11, SA#2:** update sections with approved changes.
2. **Changing and Refreshing Authenticators in the *CJISSECPOL*, Spring 2024, APB#11, SA#3:** clarifies which authenticator type requires annual changing and clarifies the use of a “banned password” list.
3. **Modernizing System and Services Acquisition (SA) in the *CJISSECPOL*, Spring 2024, APB#11, SA#5:** add definitions and modernize the CJIS Security Policy requirements for:

- System and Services Acquisition Policy and Procedures**
- Allocation of Resources**
- System Development Lifecycle**
- Acquisition Process**
- System Documentation**
- Security and Privacy Engineering Principles**
- External System Services**
- Developer Configuration Management**
- Developer Testing and Evaluation**
- Developer Process, Standards, and Tools**

4. **Modernizing Supply Chain and Risk Management (SR) in the *CJISSECPOL*, Spring 2024, APB#11, SA#6:** modernize the CJIS Security Policy requirements for

- Supply Chain Risk Management Policy and Procedures**
- Supply Chain Risk Management Plan**
- Acquisition Strategies, Tools, and Methods**
- Notification Agreements**
- Inspection of Systems or Components**
- Component Disposal**

5. **Modernizing Personnel Security (PS) in the *CJISSECPOL*, Spring 2024, APB#11, SA#7:** modernize the CJIS Security Policy requirements for

- Personnel Security Policy and Procedures**
- Position Risk Designation**
- Personnel Screening**
- Personnel Termination**
- Personnel Transfer**
- Access Agreements**
- External Personnel Security**
- Personnel Sanctions**
- Position Descriptions**

6. **Modernizing Assessment, Authorization, and Monitoring (CA) in the *CJISSECPOL*, Spring 2024, APB#11, SA#8:** modernize the CJIS Security Policy requirements for

Assessment, Authorization, and Monitoring Policy and Procedures

Control Assessments

Information Exchange

Plan of Action and Milestones

Authorization

Continuous Monitoring

Internal System Connections

7. **Remove Appendix J and K from the *CJISSECPOL*, Spring 2024, APB#11, SA#9:**
remove the indicated appendices.

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy Sections 1 - 4 (Introduction, Approach, Roles & Responsibilities, and CJI/PII)								
1.3	1.3	Relationship to Local Security Policy and Other Policies	The local agency may complement the CJIS Security Policy with a local policy, or the agency may develop their own stand-alone security policy; however, the CJIS Security Policy shall always be the minimum standard and local policy may augment, or increase the standards,...	Existing	Existing	Agency	Agency	Agency
		"	...and local policy may augment, or increase the standards, but shall not detract from the CJIS Security Policy standards.	Existing	Existing	Agency	Agency	Agency
		"	The agency shall develop, disseminate, and maintain formal, documented procedures to facilitate the implementation of the CJIS Security Policy and, where applicable, the local security policy.	Existing	Existing	Agency	Agency	Agency
		"	The policies and procedures shall be consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidance.	Existing	Existing	Agency	Agency	Agency
3.2.1	3.2.1	CJIS Systems Agencies (CSA)	The head of each CSA shall appoint a CJIS Systems Officer (CSO).	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
		"	Such decisions shall be documented and kept current.	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
3.2.2	3.2.2	CJIS Systems Officer (CSO)	Pursuant to The Bylaws for the CJIS Advisory Policy Board and Working Groups, the role of CSO shall not be outsourced.	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
		"	The CSO shall set, maintain, and enforce the following:	Existing	Existing			
3.2.2(1)	3.2.2(1)	"	1. Standards for the selection, supervision, and separation of personnel who have access to CJI.	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
3.2.2(2)	3.2.2(2)	"	2. Policy governing the operation of computers, access devices, circuits, hubs, routers, firewalls, and other components that comprise and support a telecommunications network and related CJIS systems used to process, store, or transmit CJI, guaranteeing the priority, confidentiality, integrity, and availability of service needed by the criminal justice community.	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
		"	a. Ensure appropriate use, enforce system discipline, and ensure CJIS Division operating procedures are followed by all users of the respective services and information.	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
		"	b. Ensure state/federal agency compliance with policies approved by the APB and adopted by the FBI.	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
		"	c. Ensure the appointment of the CSA ISO and determine the extent of authority to the CSA ISO.	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
		"	d. Ensure the designation of a Terminal Agency Coordinator (TAC) within each agency with device access to CJIS systems.	Existing	Existing	Agency	Agency	Agency
		"	e. Ensure each agency having access to CJI has someone designated as the Organizational Personnel with Security Responsibilities.	Existing	Existing	Agency	Agency	Agency
		"	f. Ensure the Organizational Personnel with Security Responsibilities receives enhanced security awareness training (ref. Awareness and Training (AT)).	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
		"	g. Approve access to FBI CJIS systems.	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
		"	h. Assume ultimate responsibility for managing the security of CJIS systems within their state and/or agency.	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
		"	i. Perform other related duties outlined by the user agreements with the FBI CJIS Division.	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
3.2.3(3)	3.2.3(3)	"	3. External System Services of Criminal Justice Functions: Responsibility for the	Existing	Existing	Agency	Agency	Agency
		"	a. Set and enforce standards for the selection, supervision, and termination of	Existing	Existing	Agency	Agency	Agency
		"	b. Set and enforce policy governing the operation of computers, circuits, and telecommunications terminals,	Existing	Existing	Agency	Agency	Agency
		"	c. Guarantee the priority service as determined by the CSA.	Existing	Existing	Agency	Agency	Agency

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
3.2.6	3.2.6	Contracting Agency (CA)	A CA is an agency, whether a CJA, NCJA (public), or NCJA (private), that enters into an agreement with a private contractor subject to the CJIS Security Addendum, The Security and Management Control Outsourcing Standard for Non-Channelers, of the Security and Management Control Outsourcing Standard for Channeling. The CA entering into an agreement with a contractor shall appoint an Agency Coordinator.	Existing	Existing	Agency	Agency	Agency
3.2.7	3.2.7	Agency Coordinator (AC)	The AC shall be responsible for the supervision and integrity of the system, training and continuing education of employees and operators, scheduling of initial training and testing, and certification testing and all required reports by NCIC.	Existing	Existing	Agency	Agency	Agency
		"	The AC shall :	Existing	Existing			
		"	1. Understand the communications, records capabilities, and needs of the Contractor which is accessing federal and state records through or because of its relationship with the CGA.	Existing	Existing	Agency	Agency	Agency
		"	2. Participate in related meetings and provide input and comments for system improvement.	Existing	Existing	Agency	Agency	Agency
		"	3. Receive information from the CGA (e.g., system updates) and disseminate it to appropriate Contractor employees.	Existing	Existing	Agency	Agency	Agency
		"	4. Maintain and update manuals applicable to the effectuation of the agreement, and provide them to the Contractor.	Existing	Existing	Agency	Agency	Agency
		"	5. Maintain up-to-date records of Contractor's employees who access the system, including name, date of birth, social security number, date fingerprint card(s) submitted, date security clearance issued, and date initially trained, tested, certified or recertified (if applicable).	Existing	Existing	Agency	Agency	Agency
		"	6. Train or ensure the training of Contractor personnel. If Contractor personnel access NCIC, schedule the operators for testing or a certification exam with the CSA staff, or AC staff with permission from the CSA staff. Schedule new operators for the certification exam within six (6) months of assignment. Schedule certified operators for biennial re-certification testing within thirty (30) days prior to the expiration of certification. Schedule operators for other mandated class.	Existing	Existing	Agency	Agency	Agency
		"	7. The AC will not permit an untrained/untested or non-certified Contractor employee to access CJI or systems supporting CJI where access to CJI can be gained.	Existing	Existing	Agency	Agency	Agency
		"	8. Where appropriate, ensure compliance by the Contractor with NCIC validation requirements.	Existing	Existing	Agency	Agency	Agency
		"	9. Provide completed applicant fingerprint cards on each Contractor employee who accesses the system to the CJA (or, where appropriate, CSA) for criminal background investigation prior to such employee accessing the system.	Existing	Existing	Agency	Agency	Agency
		"	10. Any other responsibility for the AC promulgated by the FBI.	Existing	Existing	Agency	Agency	Agency
3.2.8	3.2.8	CJIS System Agency Information Security Officer (CSA ISO)	The CSA ISO shall :	Existing	Existing			
		"	1. Serve as the security point of contact (POC) to the FBI CJIS Division ISO.	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
		"	2. Document technical compliance with the CJIS Security Policy with the goal to assure the confidentiality, integrity, and availability of criminal justice information to the user community throughout the CSA's user community, to include the local level.	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
		"	3. Document and provide assistance for implementing the security-related controls for the Interface Agency and its users.	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
		"	4. Establish a security incident response and reporting procedure to discover, investigate, document, and report to the CSA, the affected criminal justice agency, and the FBI CJIS Division ISO major incidents that significantly endanger the security or integrity of CJI.	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
3.2.9	3.2.9	Organizational Personnel with Security Responsibilities	Each Organizational Personnel with Security Responsibilities shall :	Existing	Existing			
		"	1. Identify who is using the CSA approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.	Existing	Existing	Agency	Agency	Agency
		"	2. Identify and document how the equipment is connected to the state system.	Existing	Existing	Agency	Agency	Agency
		"	3. Ensure that personnel security screening procedures are being followed as stated in this policy.	Existing	Existing	Agency	Agency	Agency
		"	4. Ensure the approved and appropriate security measures are in place and working as expected.	Existing	Existing	Agency	Agency	Agency
		"	5. Support policy compliance and ensure CSA ISO is promptly informed of security incidents.	Existing	Existing	Agency	Agency	Agency
3.2.10	3.2.10	FBI CJIS Division Information Security Officer (FBI CJIS ISO)	The FBI CJIS ISO shall :	Existing	Existing			
		"	1. Maintain the CJIS Security Policy.	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
		"	2. Disseminate the FBI Director approved CJIS Security Policy.	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
		"	3. Serve as a liaison with the CSA's ISO and with other personnel across the CJIS community and in this regard provide technical guidance as to the intent and implementation of operational and technical policy issues.	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
		"	4. Serve as a point-of-contact (POC) for computer incident notification and distribution of security alerts to the CSOs and ISOs.	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
		"	5. Assist with developing audit compliance guidelines as well as identifying and reconciling security-related issues.	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
		"	6. Develop and participate in information security training programs for the CSOs and ISOs, and provide a means by which to acquire feedback to measure the effectiveness and success of such training.	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
		"	7. Maintain a security policy resource center (SPRC) on FBI.gov and keep the CSOs and ISOs updated on pertinent information.	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
3.2.12	3.2.12	State Compact Officer (SCO)	Pursuant to the National Crime Prevention and Privacy Compact, each party state shall appoint a Compact Officer...	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
			...Compact Officer who shall ensure that Compact provisions and rules, procedures, and standards established by the Compact Council are complied with in their respective state.	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
4.2.1	4.2.1	Proper Access, Use, and Dissemination of CHRI	The III shall be accessed only for an authorized purpose.	Existing	Existing	Agency	Agency	Agency
		"	Further, CHRI shall only be used for an authorized purpose consistent with the purpose for which III was accessed.	Existing	Existing	Agency	Agency	Agency
4.2.2	4.2.2	Proper Access, Use, and Dissemination of NCIC Restricted Files Information	Proper access to, use, and dissemination of data from restricted files shall be consistent with the access, use, and dissemination policies concerning the III described in Title 28, Part 20, CFR, and the NCIC Operating Manual.	Existing	Existing	Agency	Agency	Agency
		"	The restricted files, which shall be protected as CHRI, are as follows:	Existing	Existing			
		"	1. Gang File	Existing	Existing	Agency	Agency	Agency
		"	2. Threat Screening Center File	Existing	Existing	Agency	Agency	Agency
		"	3. Supervised Release File	Existing	Existing	Agency	Agency	Agency
		"	4. National Sex Offender Registry File	Existing	Existing	Agency	Agency	Agency

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
4.2.2	4.2.2	Proper Access, Use, and Dissemination of NCIC Restricted Files Information (continued)	5. Historical Protection Order File of the NCIC	Existing	Existing	Agency	Agency	Agency
		"	6. Identity Theft File	Existing	Existing	Agency	Agency	Agency
		"	7. Protective Interest File	Existing	Existing	Agency	Agency	Agency
		"	8. Person With Information [PWI] data in the Missing Person Files	Existing	Existing	Agency	Agency	Agency
		"	9. Violent Person File	Existing	Existing	Agency	Agency	Agency
		"	10. NICS Denied Transaction File	Existing	Existing	Agency	Agency	Agency
4.2.3.2	4.2.3.2	For Other Authorized Purposes	Non-restricted files information shall not be disseminated commercially.	Existing	Existing	Agency	Agency	Agency
		"	Agencies shall not disseminate restricted files information for purposes other than law enforcement.	Existing	Existing	Agency	Agency	Agency
4.2.4	4.2.4	Storage	When CHRI is stored, agencies shall establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of the information.	Existing	Existing	Agency	Agency	Agency
		"	These records shall be stored for extended periods only when they are key elements for the integrity and/or utility of case files and/or criminal record files.	Existing	Existing	Agency	Agency	Agency
4.2.5.1	4.2.5.1	Justification	In addition to the use of purpose codes and logging information, all users shall provide a reason for all III inquiries whenever requested by NCIC System Managers, CSAs, local agency administrators, or their representatives.	Existing	Existing	Agency	Agency	Agency
4.3	4.3	Personally Identifiable Information (PII)	PII shall be extracted from CJI for the purpose of official business only.	Existing	Existing	Agency	Agency	Agency
		"	Agencies shall develop policies, based on state and local privacy rules, to ensure appropriate controls are applied when handling PII extracted from CJI.	Existing	Existing	Agency	Agency	Agency

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy Section 5-1: Information Exchange Agreements								
5.1	5.1	Policy Area 1: Information Exchange Agreements	The information shared through communication mediums shall be protected with appropriate security safeguards.	Existing	Existing	Agency	Agency	Agency
5.1.1	5.1.1	Information Exchange	Before exchanging CJI, agencies shall put formal agreements in place that specify security controls.	Existing	Existing	Agency	Agency	Agency
		"	Information exchange agreements for agencies sharing CJI data that is sent to and/or received from the FBI CJIS shall specify the security controls and conditions described in this document.	Existing	Existing	Agency	Agency	Agency
		"	Information exchange agreements shall be supported by documentation committing both parties to the terms of information exchange.	Existing	Existing	Agency	Agency	Agency
5.1.2	5.1.2	Monitoring, Review, and Delivery of Services	As specified in the inter-agency agreements, MCAs, and contractual agreements with private contractors, the services, reports and records provided by the service provider shall be regularly monitored and reviewed.	Existing	Existing	Agency	Agency	Agency
		"	The CJA, authorized agency, or FBI shall maintain sufficient overall control and visibility into all security aspects to include, but not limited to, identification of vulnerabilities and information security incident reporting/response.	Existing	Existing	Agency	Agency	Agency
		"	The incident reporting/response process used by the service provider shall conform to the incident reporting/response specifications provided in this policy.	Existing	Existing	Agency	Agency	Agency
5.1.2.1	5.1.2.1	Managing Changes to Service Providers	Any changes to services provided by a service provider shall be managed by the CJA, authorized agency, or FBI.	Existing	Existing	Agency	Agency	Agency
		"	Evaluation of the risks to the agency shall be undertaken based on the criticality of the data, system, and the impact of the change.	Existing	Existing	Agency	Agency	Agency

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy: Access Control (AC)								
AC-1	AC-1	POLICY AND PROCEDURES	a. Develop, document, and disseminate to: organizational personnel with access control responsibilities	Zero-cycle	P2	Agency	Both	Both
		"	1. Agency-level access control policy that:	Zero-cycle	P2	Agency	Both	Both
		"	(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Zero-cycle	P2	Agency	Both	Both
		"	(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and	Zero-cycle	P2	Agency	Both	Both
		"	2. Procedures to facilitate the implementation of the access control policy and the associated access controls;	Zero-cycle	P2	Agency	Both	Both
		"	b. Designate an individual with security responsibilities to manage the development, documentation, and dissemination of the access control policy and procedures; and	Zero-cycle	P2	Agency	Both	Both
		"	c. Review and update the current access control:	Zero-cycle	P2	Agency	Both	Both
		"	1. Policy annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI; and	Zero-cycle	P2	Agency	Both	Both
		"	2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.	Zero-cycle	P2	Agency	Both	Both
AC-2	AC-2	ACCOUNT MANAGEMENT	a. Define and document the types of accounts allowed and specifically prohibited for use within the system;	Existing	P1	Agency	Both	Both
		"	b. Assign account managers;	Existing	P1	Agency	Both	Both
		"	c. Require conditions for group and role membership;	Existing	P1	Agency	Both	Both
		"	d. Specify:	Existing	P1	Agency	Both	Both
		"	1. Authorized users of the system;	Existing	P1	Agency	Both	Both
		"	2. Group and role membership; and	Existing	P1	Agency	Both	Both
		"	3. Access authorizations (i.e., privileges) and attributes listed for each account;	10/1/2024	P1	Agency	Both	Both
		"	Attribute Name	10/1/2024	P1	Agency	Both	Both
		"	Email Address Text	10/1/2024	P1	Agency	Both	Both
		"	Employer Name	10/1/2024	P1	Agency	Both	Both
		"	Federation Id	10/1/2024	P1	Agency	Both	Both
		"	Given Name	10/1/2024	P1	Agency	Both	Both
		"	Identity Provider Id	10/1/2024	P1	Agency	Both	Both
		"	Sur Name	10/1/2024	P1	Agency	Both	Both
		"	Telephone Number	10/1/2024	P1	Agency	Both	Both
		"	Identity Provider Id	10/1/2024	P1	Agency	Both	Both
		"	Unique Subject Id	10/1/2024	P1	Agency	Both	Both
		"	Counter Terrorism Data Self Search Home Privilege Indicator	10/1/2024	P1	Agency	Both	Both
		"	Criminal History Data Self Search Home Privilege Indicator	10/1/2024	P1	Agency	Both	Both
		"	Criminal Intelligence Data Self Search Home Privilege Indicator	10/1/2024	P1	Agency	Both	Both
		"	Criminal Investigative Data Self Search Home Privilege Indicator	10/1/2024	P1	Agency	Both	Both
		"	Display Name	10/1/2024	P1	Agency	Both	Both
		"	Government Data Self Search Home Privilege Indicator	10/1/2024	P1	Agency	Both	Both
		"	Local Id	10/1/2024	P1	Agency	Both	Both
		"	NCIC Certification Indicator	10/1/2024	P1	Agency	Both	Both
		"	NDEX Privilege Indicator	10/1/2024	P1	Agency	Both	Both
		"	PCII Certification Indicator	10/1/2024	P1	Agency	Both	Both
		"	28 CFR Certification Indicator	10/1/2024	P1	Agency	Both	Both
		"	Employer ORI	10/1/2024	P1	Agency	Both	Both
		"	Employer Organization General Category Code	10/1/2024	P1	Agency	Both	Both

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
AC-2	AC-2	ACCOUNT MANAGEMENT (continued)	Employer State Code	10/1/2024	P1	Agency	Both	Both
		"	Public Safety Officer Indicator	10/1/2024	P1	Agency	Both	Both
		"	Sworn Law Enforcement Officer Indicator	10/1/2024	P1	Agency	Both	Both
		"	Authenticator Assurance Level	10/1/2024	P1	Agency	Both	Both
		"	Federation Assurance Level	10/1/2024	P1	Agency	Both	Both
		"	Identity Assurance Level	10/1/2024	P1	Agency	Both	Both
		"	Intelligence Analyst Indicator	10/1/2024	P1	Agency	Both	Both
		"	e. Require approvals by organizational personnel with account management responsibilities for requests to create accounts;	Existing	P1	Agency	Both	Both
		"	f. Create, enable, modify, disable, and remove accounts in accordance with agency policy;	Existing	P1	Agency	Both	Both
		"	g. Monitor the use of accounts;	Existing	P1	Agency	Both	Both
		"	h. Notify account managers and system/network administrators within:	10/1/2024	P1	Agency	Both	Both
		"	1. One day when accounts are no longer required;	10/1/2024	P1	Agency	Both	Both
		"	2. One day when users are terminated or transferred; and	10/1/2024	P1	Agency	Both	Both
		"	3. One day when system usage or need-to-know changes for an individual;	10/1/2024	P1	Agency	Both	Both
		"	i. Authorize access to the system based on:	Existing	P1	Agency	Both	Both
		"	1. A valid access authorization;	Existing	P1	Agency	Both	Both
		"	2. Intended system usage; and	Existing	P1	Agency	Both	Both
		"	3. Attributes as listed in AC-2(d)(3);	10/1/2024	P1	Agency	Both	Both
		"	j. Review accounts for compliance with account management requirements at least annually;	Existing	P1	Agency	Both	Both
		"	k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and	Existing	P1	Agency	Both	Both
		"	l. Align account management processes with personnel termination and transfer processes.	Existing	P1	Agency	Both	Both
AC-2(1)	AC-2(1)	(1) ACCOUNT MANAGEMENT AUTOMATED SYSTEM ACCOUNT MANAGEMENT	Support the management of system accounts using automated mechanisms including email, phone, and text notifications.	10/1/2024	P1	Agency	Both	Both
AC-2(2)	AC-2(2)	(2) ACCOUNT MANAGEMENT AUTOMATED TEMPORARY AND EMERGENCY ACCOUNT MANAGEMENT	Automatically remove temporary and emergency accounts within 72 hours.	10/1/2024	P1	Agency	Both	Both
AC-2(3)	AC-2(3)	(3) ACCOUNT MANAGEMENT DISABLE ACCOUNTS	Disable accounts within one (1) week when the accounts:	10/1/2024	P1	Agency	Both	Both
		"	(a) Have expired;	10/1/2024	P1	Agency	Both	Both
		"	(b) Are no longer associated with a user or individual;	10/1/2024	P1	Agency	Both	Both
		"	(c) Are in violation of organizational policy; or	10/1/2024	P1	Agency	Both	Both
		"	(d) Have been inactive for 90 calendar days.	10/1/2024	P1	Agency	Both	Both
AC-2(4)	AC-2(4)	(4) ACCOUNT MANAGEMENT AUTOMATED AUDIT ACTIONS	Automatically audit account creation, modification, enabling, disabling, and removal actions.	Existing	P1	Agency	Both	Both
AC-2(5)	AC-2(5)	(5) ACCOUNT MANAGEMENT INACTIVITY LOGOUT	Require that users log out when a work period has been completed.	10/1/2024	P1	Agency	Both	Both
AC-2(13)	AC-2(13)	(13) ACCOUNT MANAGEMENT DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS	Disable accounts of individuals within 30 minutes of discovery of direct threats to the confidentiality, integrity, or availability of CJI.	10/1/2024	P1	Agency	Both	Both
AC-3	AC-3	ACCESS ENFORCEMENT	Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	Existing	P1	Agency	Both	Both
AC-3(14)	AC-3(14)	(14) ACCESS ENFORCEMENT INDIVIDUAL ACCESS	Provide automated or manual processes to enable individuals to have access to elements of their personally identifiable information.	Existing	P1	Agency	Both	Both

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
AC-4	AC-4	INFORMATION FLOW ENFORCEMENT	Enforce approved authorizations for controlling the flow of information within the system and between connected systems by preventing CJI from being transmitted unencrypted across the public network, blocking outside traffic that claims to be from within the agency, and not passing any web requests to the public network that are not from agency controlled or internal boundary protection devices (e.g., proxies, gateways, firewalls, or routers).	Existing	P1	Agency	Both	Both
AC-5	AC-5	SEPARATION OF DUTIES	a. Identify and document separation of duties based on specific duties, operations, or information systems, as necessary, to mitigate risk to CJI; and	Existing	P1	Agency	Both	Both
		"	b. Define system access authorizations to support separation of duties.	Existing	P1	Agency	Both	Both
AC-6	AC-6	LEAST PRIVILEGE	Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.	Existing	P1	Agency	Both	Both
AC-6(1)	AC-6(1)	(1) LEAST PRIVILEGE AUTHORIZE ACCESS TO SECURITY FUNCTIONS	Authorize access for personnel including, security administrators, system and network administrators, and other privileged users with access to system control, monitoring, or administration functions (e.g., system administrators, information security personnel, maintainers, system programmers, etc.) to:	Existing	P1	Agency	Both	Both
		"	(a) Established system accounts, configured access authorizations (i.e., permissions, privileges), set events to be audited, set intrusion detection parameters, and other security functions; and	Existing	P1	Agency	Both	Both
		"	(b) Security-relevant information in hardware, software, and firmware.	Existing	P1	Agency	Both	Both
AC-6(2)	AC-6(2)	(2) LEAST PRIVILEGE NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS	Require that users of system accounts (or roles) with access to privileged security functions or security-relevant information (e.g., audit logs), use non-privileged accounts or roles, when accessing nonsecurity functions.	Existing	P1	Agency	Both	Both
AC-6(5)	AC-6(5)	(5) LEAST PRIVILEGE PRIVILEGED ACCOUNTS	Restrict privileged accounts on the system to privileged users.	Existing	P1	Agency	Both	Both
AC-6(7)	AC-6(7)	(7) LEAST PRIVILEGE REVIEW OF USER PRIVILEGES	a. Reviews annually the privileges assigned to non-privileged and privileged users to validate the need for such privileges; and	Existing	P1	Agency	Both	Both
		"	b. Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs.	Existing	P1	Agency	Both	Both
AC-6(9)	AC-6(9)	(9) LEAST PRIVILEGE LOG USE OF PRIVILEGED FUNCTIONS	Log the execution of privileged functions.	Existing	P1	Agency	Both	Both
AC-6(10)	AC-6(10)	(10) LEAST PRIVILEGE PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS	Prevent non-privileged users from executing privileged functions.	Existing	P1	Agency	Both	Both
AC-7	AC-7	UNSUCCESSFUL LOGON ATTEMPTS	a. Enforce a limit of five (5) consecutive invalid logon attempts by a user during a 15-minute time period; and	Existing	P3	Agency	Both	Both
		"	b. Automatically lock the account or node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.	Existing	P3	Agency	Both	Both
AC-8	AC-8	SYSTEM USE NOTIFICATION	a. Display a system use notification message to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that:	Existing	P2	Agency	Both	Both
		"	1. Users are accessing a restricted information system;	Existing	P2	Agency	Both	Both
		"	2. System usage may be monitored, recorded, and subject to audit;	Existing	P2	Agency	Both	Both

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
AC-8	AC-8	SYSTEM USE NOTIFICATION (continued)	3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and	Existing	P2	Agency	Both	Both
		"	4. Use of the system indicates consent to monitoring and recording;	Existing	P2	Agency	Both	Both
		"	b. Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system; and	Existing	P2	Agency	Both	Both
		"	c. For publicly accessible systems:	Existing	P2	Agency	Both	Both
		"	1. Display system use information consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines, before granting further access to the publicly accessible system;	Existing	P2	Agency	Both	Both
		"	2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and	Existing	P2	Agency	Both	Both
		"	3. Include a description of the authorized uses of the system.	Existing	P2	Agency	Both	Both
AC-11	AC-11	DEVICE LOCK	a. Prevent further access to the system by initiating a device lock after a maximum of 30 minutes of inactivity and requiring the user to initiate a device lock before leaving the system unattended.	Existing	P4	Agency	Both	Both
		"	NOTE: In the interest of safety, devices that are: (1) part of a criminal justice conveyance; or (2) used to perform dispatch functions and located within a physically secure location; or (3) terminals designated solely for the purpose of receiving alert notifications (i.e., receive only terminals or ROT) used within physically secure location facilities that remain staffed when in operation, are exempt from this requirement.	Existing	P4	Agency	Both	Both
		"	b. Retain the device lock until the user reestablishes access using established identification and authentication procedures.	Existing	P4	Agency	Both	Both
AC-11(1)	AC-11(1)	(1) DEVICE LOCK PATTERN-HIDING DISPLAYS	Conceal, via the device lock, information previously visible on the display with a publicly viewable image.	Existing	P4	Agency	Both	Both
AC-12	AC-12	SESSION TERMINATION	Automatically terminate a user session after a user has been logged out.	Zero-cycle	P3	Agency	Both	Both
AC-14	AC-14	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION	a. Identify any specific user actions that can be performed on the system without identification or authentication consistent with organizational mission and business functions; and	Zero-cycle	P4	Agency	Both	Both
		"	b. Document and provide supporting rationale in the security plan for the system, user actions not requiring identification or authentication.	Zero-cycle	P4	Agency	Both	Both
AC-17	AC-17	REMOTE ACCESS	a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and	Existing	P1	Agency	Both	Both
		"	b. Authorize each type of remote access to the system prior to allowing such connections.	Existing	P1	Agency	Both	Both
AC-17(1)	AC-17(1)	(1) REMOTE ACCESS MONITORING AND CONTROL	Employ automated mechanisms to monitor and control remote access methods.	Existing	P1	Agency	Both	Both
AC-17(2)	AC-17(2)	(2) REMOTE ACCESS PROTECTION OF CONFIDENTIALITY AND INTEGRITY USING ENCRYPTION	Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.	Existing	P1	Agency	Both	Both
AC-17(3)	AC-17(3)	(3) REMOTE ACCESS MANAGED ACCESS CONTROL POINTS	Route remote accesses through authorized and managed network access control points.	Existing	P1	Agency	Both	Both
AC-17(4)	AC-17(4)	(4) REMOTE ACCESS PRIVILEGED COMMANDS AND ACCESS	(a) Authorize the execution of privileged commands and access to security-relevant information via remote access only in a format that provides assessable evidence and for the following needs: compelling operational needs; and	Existing	P1	Agency	Both	Both
		"	(b) Document the rationale for remote access in the security plan for the system.	Existing	P1	Agency	Both	Both

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
AC-18	AC-18	WIRELESS ACCESS	a. Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access; and	Existing	P2	Agency	Both	Both
		"	b. Authorize each type of wireless access to the system prior to allowing such connections.	Existing	P2	Agency	Both	Both
AC-18(1)	AC-18(1)	(1) WIRELESS ACCESS AUTHENTICATION AND ENCRYPTION	Protect wireless access to the system using authentication of authorized users and agency-controlled devices, and encryption.	Existing	P2	Agency	Both	Both
AC-18(3)	AC-18(3)	(3) WIRELESS ACCESS DISABLE WIRELESS NETWORKING	Disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment.	Existing	P2	Agency	Both	Both
AC-19	AC-19	ACCESS CONTROL FOR MOBILE DEVICES	a. Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas; and	Existing	P2	Agency	Both	Both
		"	b. Authorize the connection of mobile devices to organizational systems.	Existing	P2	Agency	Both	Both
AC-19(5)	AC-19(5)	(5) ACCESS CONTROL FOR MOBILE DEVICES FULL DEVICE OR CONTAINER-BASED ENCRYPTION	Employ full-device encryption to protect the confidentiality and integrity of information on full- and limited-feature operating system mobile devices authorized to process, store, or transmit CJI.	Existing	P2	Agency	Both	Both
AC-20	AC-20	USE OF EXTERNAL SYSTEMS	a. Establish agency-level policies governing the use of external systems consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to:	Existing	P1	Agency	Both	Both
		"	1. Access the system from external systems; and	Existing	P1	Agency	Both	Both
		"	2. Process, store, or transmit organization-controlled information using external systems; or	Existing	P1	Agency	Both	Both
		"	b. Prohibit the use of personally-owned information systems including mobile devices (i.e., bring your own device [BYOD]) and publicly accessible systems for accessing, processing, storing, or transmitting CJI.	10/1/2024	P1	Agency	Both	Both
AC-20(1)	AC-20(1)	(1) USE OF EXTERNAL SYSTEMS LIMITS ON AUTHORIZED USE	Permit authorized individuals to use an external system to access the system or to process, store, or transmit organization-controlled information only after:	Existing	P1	Agency	Both	Both
		"	(a) Verification of the implementation of controls on the external system as specified in the organization's security and privacy policies and security and privacy plans; or	Existing	P1	Agency	Both	Both
		"	(b) Retention of approved system connection or processing agreements with the organizational entity hosting the external system.	Existing	P1	Agency	Both	Both
AC-20(2)	AC-20(2)	(2) USE OF EXTERNAL SYSTEMS PORTABLE STORAGE DEVICES — RESTRICTED USE	Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems.	Existing	P1	Agency	Both	Both
AC-21	AC-21	INFORMATION SHARING	a. Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions as defined in an executed information exchange agreement; and	Existing	P3	Agency	Both	Both
		"	b. Employ attribute-based access control (see AC-2(d)(3)) or manual processes as defined in information exchange agreements to assist users in making information sharing and collaboration decisions.	Existing	P3	Agency	Both	Both

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
AC-22	AC-22	PUBLICLY ACCESSIBLE CONTENT	a. Designate individuals authorized to make information publicly accessible;	Zero-cycle	P4	Agency	Both	Both
		"	b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information;	Zero-cycle	P4	Agency	Both	Both
		"	c. Review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included; and	Zero-cycle	P4	Agency	Both	Both
		"	d. Review the content on the publicly accessible system for nonpublic information quarterly and remove such information, if discovered.	Zero-cycle	P4	Agency	Both	Both

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy: Awareness and Training (AT)								
5.2: AT-1	AT-1	Policy and Procedures	a. Develop, document, and disseminate to all personnel when their unescorted logical or physical access to any information system results in the ability, right, or privilege to view, modify, or make use of unencrypted CJI:	Zero-cycle	P2	Both	Both	Both
		"	1. Organization-level awareness and training policy that:	Zero-cycle	P2	Both	Both	Both
		"	(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Zero-cycle	P2	Both	Both	Both
		"	(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and	Zero-cycle	P2	Both	Both	Both
		"	2. Procedures to facilitate the implementation of the awareness and training policy and the associated awareness and training controls;	Zero-cycle	P2	Both	Both	Both
		"	b. Designate organizational personnel with information security awareness and training responsibilities to manage the development, documentation, and dissemination of the awareness and training policy nd procedures; and	Zero-cycle	P2	Both	Both	Both
		"	c. Review and update the current awareness and training:	Zero-cycle	P2	Both	Both	Both
		"	1. Policy annually and following changes in the information system operating environment, when security incidents occur, or when changes to the CJIS Security Policy are made; and	Zero-cycle	P2	Both	Both	Both
		"	2. Procedures annually and following changes in the information system operating environment, when security incidents occur, or when changes to the CJIS Security Policy are made.	Zero-cycle	P2	Both	Both	Both
5.2: AT-2	AT-2	Literacy Training and Awareness	a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors):	Existing	P2	Both	Both	Both
		"	1. As part of initial training for new users prior to accessing CJI and annually thereafter; and	Existing	P2	Both	Both	Both
		"	2. When required by system changes or within 30 days of any security event for individuals involved in the event;	Existing	P2	Both	Both	Both
		"	b. Employ one or more of the following techniques to increase the security and privacy awareness of system users:	Existing	P2	Both	Both	Both
		"	1. Displaying posters	Existing	P2	TBD	TBD	TBD
		"	2. Offering supplies inscribed with security and privacy reminders	Existing	P2	TBD	TBD	TBD
		"	3. Displaying logon screen messages	Existing	P2	TBD	TBD	TBD
		"	4. Generating email advisories or notices from organizational officials	Existing	P2	TBD	TBD	TBD
		"	5. Conducting awareness events	Existing	P2	TBD	TBD	TBD
		"	c. Update literacy training and awareness content annually and following changes in the information system operating environment, when security incidents occur, or when changes are made in the CJIS Security Policy; and	Existing	P2	Both	Both	Both
5.2: AT-2 (2)	AT-2 (2)	LITERACY TRAINING AND AWARENESS INSIDER THREAT	Provide literacy training on recognizing and reporting potential indicators of insider threat.	Existing	P2	Both	Both	Both
		5.2: AT-2 (3)	AT-2 (3)	LITERACY TRAINING AND AWARENESS SOCIAL ENGINEERING AND MINING	Provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining.	Existing	P2	Both
5.2: AT-3	AT-3	ROLE-BASED TRAINING	a. Provide role-based security and privacy training to personnel with the following roles and responsibilities:	Existing	P2	Both	Both	Both
		"	· All individuals with unescorted access to a physically secure location;	Existing	P2	Both	Both	Both

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
5.2: AT-3	AT-3	ROLE-BASED TRAINING (continued)	· General User: A user, but not a process, who is authorized to use an information system;	Existing	P2	Both	Both	Both
		"	· Privileged User: A user that is authorized (and, therefore, trusted) to perform security-relevant functions that general users are not authorized to perform:	Existing	P2	Both	Both	Both
		"	1. Before authorizing access to the system, information, or performing assigned duties, and annually thereafter; and	Existing	P2	Both	Both	Both
		"	2. When required by system changes;	Existing	P2	Both	Both	Both
		"	b. Update role-based training content annually and following audits of the CSA and local agencies ; changes in the information system operating environment; security incidents; or when changes are made to the CJIS Security Policy;	Existing	P2	Both	Both	Both
		"	c. Incorporate lessons learned from internal or external security incidents or breaches into role-based training;	Existing	P2	Both	Both	Both
		"	d. Incorporate the minimum following topics into the appropriate role-based training content:	Existing	P2	Both	Both	Both
		"	1. All individuals with unescorted access to a physically secure location:	Existing	P2			
		"	a. Access, Use and Dissemination of Criminal History Record Information (CHRI), NCIC Restricted Files Information, and NCIC Non-Restricted Files Information Penalties	Existing	P2	Both	Both	Both
		"	b. Reporting Security Events	Existing	P2	Both	Both	Both
		"	c. Training	Existing	P2	Both	Both	Both
		"	d. System Use Notification	Existing	P2	Both	Both	Both
		"	e. Physical Access Authorizations	Existing	P2	Both	Both	Both
		"	f. Physical Access Control	Existing	P2	Both	Both	Both
		"	g. Monitoring Physical Access	Existing	P2	Both	Both	Both
		"	h. Visitor Control	Existing	P2	Both	Both	Both
		"	i. Personnel Sanctions	Existing	P2	Both	Both	Both
		"	2. General User: A user, but not a process, who is authorized to use an information system. In addition to AT-3 (d) (1) above, include the following topics:	Existing	P2			
		"	a. Criminal Justice Information	Existing	P2	Both	Both	Both
		"	b. Proper Access, Use, and Dissemination of NCIC Non-Restricted Files Information	Existing	P2	Both	Both	Both
		"	c. Personally Identifiable Information	Existing	P2	Both	Both	Both
		"	d. Information Handling	Existing	P2	Both	Both	Both
		"	e. Media Storage	Existing	P2	Both	Both	Both
		"	f. Media Access	Existing	P2	Both	Both	Both
		"	g. Audit Monitoring, Analysis, and Reporting	Existing	P2	Both	Both	Both
		"	h. Access Enforcement	Existing	P2	Both	Both	Both
		"	i. Least Privilege	Existing	P2	Both	Both	Both
		"	j. System Access Control	Existing	P2	Both	Both	Both
		"	k. Access Control Criteria	Existing	P2	Both	Both	Both
		"	l. System Use Notification	Existing	P2	Both	Both	Both
		"	m. Session Lock	Existing	P2	Both	Both	Both
		"	n. Personally Owned Information Systems	Existing	P2	Both	Both	Both
		"	o. Password	Existing	P2	Both	Both	Both
		"	p. Access Control for Display Medium	Existing	P2	Both	Both	Both
		"	q. Encryption	Existing	P2	Both	Both	Both

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
5.2: AT-3	AT-3	ROLE-BASED TRAINING (continued)	r. Malicious Code Protection	Existing	P2	Both	Both	Both
		"	s. Spam and Spyware Protection	Existing	P2	Both	Both	Both
		"	t. Cellular Devices	Existing	P2	Both	Both	Both
		"	u. Mobile Device Management	Existing	P2	Both	Both	Both
		"	v. Wireless Device Risk Mitigations	Existing	P2	Both	Both	Both
		"	w. Wireless Device Malicious Code Protection	Existing	P2	Both	Both	Both
		"	x. Literacy Training and Awareness/Social Engineering and Mining	Existing	P2	Both	Both	Both
		"	y. Identification and Authentication (Organizational Users)	Existing	P2	Both	Both	Both
		"	z. Media Protection	Existing	P2	Both	Both	Both
		"	3. Privileged User: A user that is authorized (and, therefore, trusted) to perform security-relevant functions that general users are not authorized to perform. In addition to AT-3 (d) (1) and (2) above, include the following topics:	Existing	P2			
		"	a. Access Control	Existing	P2	Both	Both	Both
		"	b. System and Communications Protection and Information Integrity	Existing	P2	Both	Both	Both
		"	c. Patch Management	Existing	P2	Both	Both	Both
		"	d. Data backup and storage—centralized or decentralized approach	Existing	P2	Both	Both	Both
		"	e. Most recent changes to the CJIS Security Policy	Existing	P2	Both	Both	Both
		"	4. Organizational Personnel with Security Responsibilities: Personnel with the responsibility to ensure the confidentiality, integrity, and availability of CJI and the implementation of technology in a manner compliant with the CJISSECPOL. In addition to AT-3 (d) (1), (2), and (3) above, include the following topics:	Existing	P2			
		"	a. Local Agency Security Officer Role	Existing	P2	Both	Both	Both
		"	b. Authorized Recipient Security Officer Role	Zero-cycle	P2	Both	Both	Both
		"	c. Additional state/local/tribal/federal agency LASO roles and responsibilities	Existing	P2	Both	Both	Both
		"	d. Summary of audit findings from previous state audits of local agencies	Existing	P2	Both	Both	Both
		"	e. Findings from the last FBI CJIS Division audit	Existing	P2	Both	Both	Both
5.2: AT-3 (5)	AT-3 (5)	ROLE-BASED TRAINING PROCESSING PERSONALLY IDENTIFIABLE INFORMATION	Provide all personnel when their unescorted logical or physical access to any information system results in the ability, right, or privilege to view, modify, or make use of unencrypted CJI with initial and annual training in the employment and operation of personally identifiable information processing and transparency controls.	Zero-cycle	P2	Both	Both	Both
5.2: AT-4	AT-4	TRAINING RECORDS	a. Document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training; and	Existing	P4	Both	Both	Both
		"	b. Retain individual training records for a minimum of three years.	Existing	P4	Both	Both	Both

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy: Audit and Accountability								
AU-1	AU-1	POLICY AND PROCEDURES	a. Develop, document, and disseminate to organizational personnel with audit and accountability responsibilities:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. Agency and system-level audit and accountability policy that:	Zero-cycle	P2	TBD	TBD	TBD
		"	(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Zero-cycle	P2	TBD	TBD	TBD
		"	(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and	Zero-cycle	P2	TBD	TBD	TBD
		"	2. Procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls;	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Designate organizational personnel with information security responsibilities to manage the development, documentation, and dissemination of the audit and accountability policy and procedures; and	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Review and update the current audit and accountability:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. Policy annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI; and	Zero-cycle	P2	TBD	TBD	TBD
		"	2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.	Zero-cycle	P2	TBD	TBD	TBD
AU-2	AU-2	EVENT LOGGING	a. Identify the types of events that the system is capable of logging in support of the audit function: authentication, file use, user/group management, events sufficient to establish what occurred, the sources of events, outcomes of events, and operational transactions (e.g., NCIC, III);	Existing	P2	Both	Both	Service Provider
		"	b. Coordinate the event logging function with other organizational entities requiring audit- related information to guide and inform the selection criteria for events to be logged;	Existing	P2	Both	Both	Service Provider
		"	c. Specify the following event types for logging within the system:	Existing	P2	Both	Both	Service Provider
		"	All successful and unsuccessful:	Existing	P2	Both	Both	Service Provider
		"	1. System log-on attempts	Existing	P2	Both	Both	Service Provider
		"	2. Attempts to use:	Existing	P2	Both	Both	Service Provider
		"	a. Access permission on a user account, file, directory, or other system resource;	Existing	P2	Both	Both	Service Provider
		"	b. Create permission on a user account, file, directory, or other system resource;	Existing	P2	Both	Both	Service Provider
		"	c. Write permission on a user account, file, directory, or other system resource;	Existing	P2	Both	Both	Service Provider
		"	d. Delete permission on a user account, file, directory, or other system resource;	Existing	P2	Both	Both	Service Provider
		"	e. Change permission on a user account, file, directory, or other system resource.	Existing	P2	Both	Both	Service Provider
		"	3. Attempts to change account passwords	Existing	P2	Both	Both	Service Provider
		"	4. Actions by privileged accounts (i.e., root, Oracle, DBA, admin, etc.)	Existing	P2	Both	Both	Service Provider

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
AU-2	AU-2	EVENT LOGGING (continued)	5. Attempts for users to:	Existing	P2	Both	Both	Service Provider
		"	a. Access the audit log file;	Existing	P2	Both	Both	Service Provider
		"	b. Modify the audit log file;	Existing	P2	Both	Both	Service Provider
		"	c. Destroy the audit log file;	Existing	P2	Both	Both	Service Provider
		"	d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and	Existing	P2	Both	Both	Service Provider
		"	e. Review and update the event types selected for logging annually.	Existing	P2	Both	Both	Service Provider
AU-3	AU-3	CONTENT OF AUDIT RECORDS	Ensure that audit records contain information that establishes the following:	Existing	P2	Both	Both	Service Provider
		"	a. What type of event occurred;	Existing	P2	Both	Both	Service Provider
		"	b. When the event occurred;	Existing	P2	Both	Both	Service Provider
		"	c. Where the event occurred;	Existing	P2	Both	Both	Service Provider
		"	d. Source of the event;	Existing	P2	Both	Both	Service Provider
		"	e. Outcome of the event; and	Existing	P2	Both	Both	Service Provider
		"	f. Identity of any individuals, subjects, or objects/entities associated with the event.	Existing	P2	Both	Both	Service Provider
AU-3 (1)	AU-3 (1)	(1) CONTENT OF AUDIT RECORDS ADDITIONAL AUDIT INFORMATION	Generate audit records containing the following additional information:	Existing	P2	Both	Both	Service Provider
		"	a. Session, connection, transaction, and activity duration;	Existing	P2	Both	Both	Service Provider
		"	b. Source and destination addresses;	Existing	P2	Both	Both	Service Provider
		"	c. Object or filename involved; and	Existing	P2	Both	Both	Service Provider
		"	d. Number of bytes received and bytes sent (for client-server transactions) in the audit records for audit events identified by type, location, or subject.	Existing	P2	Both	Both	Service Provider
		"	e. The III portion of the log shall clearly identify:	Existing	P2	Both	Both	Service Provider
		"	1. The operator	Existing	P2	Agency	Agency	Agency
		"	2. The authorized receiving agency	Existing	P2	Agency	Agency	Agency
		"	3. The requestor	Existing	P2	Agency	Agency	Agency
AU-3 (3)	AU-3 (3)	(3) CONTENT OF AUDIT RECORDS LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS	Limit personally identifiable information contained in audit records to the following elements identified in the privacy risk assessment: minimum PII necessary to achieve the purpose for which it is collected (see Section 4.3).	Zero-cycle	P2	TBD	TBD	TBD
		AU-4	Allocate audit log storage capacity to accommodate the collection of audit logs to meet retention requirements (AU-11).	Zero-cycle	P2	TBD	TBD	TBD

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
AU-5	AU-5	RESPONSE TO AUDIT LOGGING PROCESS FAILURES	a. Alert organizational personnel with audit and accountability responsibilities and system/network administrators within one (1) hour in the event of an audit logging process failure; and	Existing	P2	Both	Both	Both
		"	b. Take the following additional actions: restart all audit logging processes and verify system(s) are logging properly.	Existing	P2	Both	Both	Both
AU-6	AU-6	AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING	a. Review and analyze system audit records weekly for indications of inappropriate or unusual activity and the potential impact of the inappropriate or unusual activity;	Existing	P2	Both	Both	Both
		"	b. Report findings to organizational personnel with audit review, analysis, and reporting responsibilities and organizational personnel with information security and privacy responsibilities; and	Existing	P2	Both	Both	Both
		"	c. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.	Existing	P2	Both	Both	Both
AU-6 (1)	AU-6 (1)	(1) AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING AUTOMATED PROCESS INTEGRATION	Integrate audit record review, analysis, and reporting processes using automated mechanisms.	Zero-cycle	P2	TBD	TBD	TBD
AU-6 (3)	AU-6 (3)	(3) AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING CORRELATE AUDIT RECORD REPOSITORIES	Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.	Zero-cycle	P2	TBD	TBD	TBD
AU-7	AU-7	AUDIT RECORD REDUCTION AND REPORT GENERATION	a. Supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents; and	Zero-cycle	P3	TBD	TBD	TBD
		"	b. Does not alter the original content or time ordering of audit records.	Zero-cycle	P3	TBD	TBD	TBD
AU-7 (1)	AU-7 (1)	(1) AUDIT RECORD REDUCTION AND REPORT GENERATION AUTOMATIC PROCESSING	Provide and implement the capability to process, sort, and search audit records for events of interest based on the following content: information included in AU-3.	Zero-cycle	P3	TBD	TBD	TBD
AU-8	AU-8	TIME STAMPS	a. Use internal system clocks to generate time stamps for audit records;	Existing	P2	Both	Both	Service Provider
		"	b. Record time stamps for audit records that meet hundredths of a second (i.e., hh:mm:ss:00) interval and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.	Existing	P2	Both	Both	Service Provider
AU-9	AU-9	PROTECTION OF AUDIT INFORMATION	a. Protect audit information and audit logging tools from unauthorized access, modification, and deletion; and	Existing	P2	Both	Both	Service Provider
		"	b. Alert organizational personnel with audit and accountability responsibilities, organizational personnel with information security and privacy responsibilities, and system/network administrators upon detection of unauthorized access, modification, or deletion of audit information.	Existing	P2	Both	Both	Service Provider
AU-9 (4)	AU-9 (4)	(4) PROTECTION OF AUDIT INFORMATION ACCESS BY SUBSET OF PRIVILEGED USERS	Authorize access to management of audit logging functionality to only organizational personnel with audit and accountability responsibilities, organizational personnel with information security and privacy responsibilities, and system/network administrators.	Zero-cycle	P2	TBD	TBD	TBD
AU-11	AU-11	AUDIT RECORD RETENTION	Retain audit records for a minimum of one (1) year or until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.	Existing	P4	Both	Both	Service Provider

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
AU-12	AU-12	AUDIT RECORD GENERATION	a. Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on all systems generating required audit logs;	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Allow organizational personnel with audit record generation responsibilities, organizational personnel with information security and privacy responsibilities, and system/network administrators to select the event types that are to be logged by specific components of the system; and	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Generate audit records for the event types defined in AU-2c that include the audit record content defined in AU-3.	Zero-cycle	P2	TBD	TBD	TBD

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy: Assessment, Authorization, and Monitoring (CA)								
	CA-1	POLICY AND PROCEDURES	a. Develop, document, and disseminate to organizational personnel with assessment, authorization, and monitoring policy responsibilities:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. An assessment, authorization, and monitoring policy that:	Zero-cycle	P2	TBD	TBD	TBD
		"	(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Zero-cycle	P2	TBD	TBD	TBD
		"	(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and	Zero-cycle	P2	TBD	TBD	TBD
		"	2. Procedures to facilitate the implementation of the assessment, authorization, and monitoring policy and the associated assessment, authorization, and monitoring controls;	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Designate organizational personnel with security responsibilities to manage the development, documentation, and dissemination of the assessment, authorization, and monitoring policy and procedures; and	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Review and update the current assessment, authorization, and monitoring:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. Policy annually and following changes to the assessment criteria and	Zero-cycle	P2	TBD	TBD	TBD
		"	2. Procedures annually and following changes to the assessment criteria.	Zero-cycle	P2	TBD	TBD	TBD
	CA-2	CONTROL ASSESSMENTS	a. Select the appropriate assessor or assessment team for the type of assessment to be conducted;	Zero-cycle	P3	TBD	TBD	TBD
		"	b. Develop a control assessment plan that describes the scope of the assessment including:	Zero-cycle	P3	TBD	TBD	TBD
		"	1. Controls and control enhancements under assessment;	Zero-cycle	P3	TBD	TBD	TBD
		"	2. Assessment procedures to be used to determine control effectiveness; and	Zero-cycle	P3	TBD	TBD	TBD
		"	3. Assessment environment, assessment team, and assessment roles and responsibilities;	Zero-cycle	P3	TBD	TBD	TBD
		"	c. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the	Zero-cycle	P3	TBD	TBD	TBD
		"	d. Assess the controls in the system and its environment of operation and any controls that have been impacted by evolving threats at least once every three years to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements;	Zero-cycle	P3	TBD	TBD	TBD
		"	e. Produce a control assessment report that documents the results of the assessment; and	Zero-cycle	P3	TBD	TBD	TBD
		"	f. Provide the results of the control assessment report to the individual who executed the CJIS User Agreement or is in contract with the FBI.	Zero-cycle	P3	TBD	TBD	TBD
	CA-2(1)	(1) CONTROL ASSESSMENTS INDEPENDENT ASSESSORS	Employ independent assessors or assessment teams to conduct control assessments.	Zero-cycle	P3	TBD	TBD	TBD
	5.1.1	CA-3	INFORMATION EXCHANGE	a. Approve and manage the exchange of information between the agency system and external systems using the following agreements when applicable;	Existing	P2	Agency	Agency
5.1.1.2	"		1. Executed CJIS User Agreements	Existing	P2	Agency	Agency	Agency
	"		a. Each CSA, SIB, or IA shall execute a signed written agreement (see Appendix D.1) with the FBI CJIS Division stating their willingness to demonstrate conformity with the CJISSECPOL before accessing and consuming CJIS systems and services as set forth in the agreement.	Existing	P2	Agency	Agency	Agency
	"		b. The agreement shall include the standards, audit, and sanctions governing utilization of CJIS systems and services.	Existing	P2	Agency	Agency	Agency
	"		c. The FBI CJIS Division is authorized to periodically test the ability to penetrate the FBI's network through the external connection or system upon proper notification of all signatories in the user agreement.	Existing	P2	Agency	Agency	Agency

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
5.1.1.3	CA-3	INFORMATION EXCHANGE (continued)	2. Criminal Justice Agency User Agreements	Existing	P2	Agency	Agency	Agency
		"	a. Any CJA receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA providing the access.	Existing	P2	Agency	Agency	Agency
		"	b. The written agreement shall specify the FBI CJIS systems and services to which the agency will have access, and the FBI CJIS Division policies to which the agency must adhere. These agreements shall include:	Existing	P2	Agency	Agency	Agency
		"	i. Audit	Existing	P2	Agency	Agency	Agency
		"	ii. Dissemination	Existing	P2	Agency	Agency	Agency
		"	iii. Hit confirmation	Existing	P2	Agency	Agency	Agency
		"	iv. Logging	Existing	P2	Agency	Agency	Agency
		"	v. Quality Assurance (QA)	Existing	P2	Agency	Agency	Agency
		"	vi. Screening (Criminal Justice Employment)	Existing	P2	Agency	Agency	Agency
		"	vii. Security	Existing	P2	Agency	Agency	Agency
		"	viii. Timeliness	Existing	P2	Agency	Agency	Agency
		"	ix. Training	Existing	P2	Agency	Agency	Agency
		"	x. Use of the system	Existing	P2	Agency	Agency	Agency
		"	xi. Validation	Existing	P2	Agency	Agency	Agency
5.1.1		"	3. Agreements for Noncriminal Justice Use of CHRI	Existing	P2	Agency	Agency	Agency
5.1.1.6		"	A CJA, NCJA (public), or NCJA (private) designated to request civil fingerprint-based background checks, with full consent of the individual to whom the background check is taking place, for noncriminal justice functions, shall be eligible for access to CHRI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. The CJA, NCJA (public), or NCJA (private) receiving access to CHRI shall enter into signed written agreements with the appropriate signatory authority of the CSA, SIB, or authorized agency providing the access. The written agreement shall specify the policies to which the agency must adhere, which includes all pertinent areas of the CJISSECPOL. Each NCJA that directly access FBI systems shall allow the FBI to periodically test the ability to penetrate the FBI's network through the external connection or system. A CJA, NCJA (public), or NCJA (private) authorized to access CHRI for noncriminal justice functions pursuant to federal law or state statute approved by the U.S. Attorney General (defined by the Compact Council as an Authorized Recipient), cannot make CHRI available to another governmental agency, nongovernmental agency, or private contractor to perform noncriminal justice administrative functions without implementation of one of the following:	Existing	P2	Agency	Agency	Agency
5.1.1.8		"	a. Security and Management Control Outsourcing Standard for Non-Channelers. Implementation is applicable to noncriminal justice administrative functions that do not require a direct connection to the FBI for submission of fingerprints and receipt of CHRI. Examples include making fitness determinations, processing, storing, or destroying documents, and maintaining IT platforms that do not connect to CJIS systems. Prior to implementation, Authorized Recipients must request and receive written permission from the State Compact Officer, Chief Administrator of the state's criminal history record repository, or the FBI Compact Officer, as applicable.	Existing	P2	Agency	Agency	Agency

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
5.1.1.7	CA-3	INFORMATION EXCHANGE (continued)	b. Security and Management Control Outsourcing Standard for Channeling. Implementation is applicable only to Channeling functions performed by an FBI-approved Channeler that require a direct connection to the FBI for submission of fingerprints and receipt of CHRI. Prior to implementation, Authorized Recipients must request and receive written permission from the State Compact Officer, Chief Administrator of the state's criminal history record repository, or the FBI Compact Officer, as applicable.	Existing	P2	Agency	Agency	Agency
5.1.1.4		"	c. Management Control Agreement or Security Addendum (see Appendix H) pursuant to Title 28, C.F.R., Section 20.33 (a) (6) or (7). Although by regulation implementation of a Management Control Agreement or the Security Addendum is applicable to the administration of criminal justice pursuant to that agreement performed on behalf of CJAs, under very limited circumstances, implementation may also be applicable to CJAs that obtain and use CHRI for noncriminal justice purposes. Implementation for noncriminal justice purposes is only applicable when another governmental agency or private contractor performs both criminal justice and noncriminal justice administrative functions involving access to CHRI on behalf of the CJA. It is important to note that if the servicing governmental agency or private contractor solely performs noncriminal justice administrative functions, then the CJA would be required to implement the Security and Management Control Outsourcing Standard for Non-Channelers.	Existing	P2	Agency	Agency	Agency
5.1.1		"	b. Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated; and	Existing	P2	Agency	Agency	Agency
		"	c. Review and update the agreements at least triennially or when responsibilities or signatories change.	Existing	P2	Agency	Agency	Agency
5.1.3 / 5.1.4		"	d. Secondary Dissemination	Existing	P2	Agency	Agency	Agency
5.1.3		"	1. Log the dissemination of CHRI when released to another authorized agency, and that agency was not part of the releasing agency's primary information exchange agreement(s). If CJI does not contain CHRI and is not part of an information exchange agreement, then it does not need to be	Existing	P2	Agency	Agency	Agency
5.1.4		"	2. Validate the requestor of CJI in conformance with the local policy as an employee and/or contractor of a law enforcement agency or civil agency requiring the CJI to perform their mission; or a member of the public receiving CJI via authorized dissemination.	Existing	P2	Agency	Agency	Agency
		CA-5	PLAN OF ACTION AND MILESTONES	a. Develop a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and	Zero-cycle	P4	TBD	TBD
	"		b. Update existing plan of action and milestones at least every six (6) months or when new information is available based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.	Zero-cycle	P4	TBD	TBD	TBD

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
	CA-6	AUTHORIZATION	a. Assign a senior official as the responsible official for the system;	Zero-cycle	P3	TBD	TBD	TBD
		"	b. Assign the CSO, SIB Chief, or IA Official as the authorizing official for common controls available for inheritance by organizational systems;	Zero-cycle	P3	TBD	TBD	TBD
		"	c. Ensure that the authorizing official for the system, before commencing operations:	Zero-cycle	P3	TBD	TBD	TBD
		"	1. Accepts the use of common controls inherited by the system; and	Zero-cycle	P3	TBD	TBD	TBD
		"	2. Authorizes the system to operate;	Zero-cycle	P3	TBD	TBD	TBD
		"	d. Ensure that the authorizing official for common controls authorizes the use of those controls for inheritance by organizational systems;	Zero-cycle	P3	TBD	TBD	TBD
		"	e. Update the authorizations at least every three (3) years.	Zero-cycle	P3	TBD	TBD	TBD
	CA-7	CONTINUOUS MONITORING	Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes:	12/27/2024	P1	TBD	TBD	TBD
		"	a. Establishing the following system-level metrics to be monitored:	12/27/2024	P1	TBD	TBD	TBD
		"	1. AC-2(g) Account Management	12/27/2024	P1	TBD	TBD	TBD
		"	2. AC-17(1) Remote Access Monitoring and Control	12/27/2024	P1	TBD	TBD	TBD
		"	3. AT-4(a) Training Records	12/27/2024	P1	TBD	TBD	TBD
		"	4. CM-3(f) Configuration Change Control	12/27/2024	P1	TBD	TBD	TBD
		"	5. CM-6(d) Configuration Settings	12/27/2024	P1	TBD	TBD	TBD
		"	6. CM-11(c) User-Installed Software	12/27/2024	P1	TBD	TBD	TBD
		"	7. IR-5 Incident Monitoring	12/27/2024	P1	TBD	TBD	TBD
		"	8. MA-2(b) Controlled Maintenance	12/27/2024	P1	TBD	TBD	TBD
		"	9. MA-3(a) Maintenance Tool	12/27/2024	P1	TBD	TBD	TBD
		"	10. MA-4(a) Nonlocal Maintenance	12/27/2024	P1	TBD	TBD	TBD
		"	11. PE-3(d) Physical Access Control	12/27/2024	P1	TBD	TBD	TBD
		"	12. PE-6 Monitoring Physical Access	12/27/2024	P1	TBD	TBD	TBD
		"	13. PE-14(b) Environmental Controls	12/27/2024	P1	TBD	TBD	TBD
		"	14. PE-16 Delivery and Removal	12/27/2024	P1	TBD	TBD	TBD
		"	15. PS-7(e) External Personnel Security	12/27/2024	P1	TBD	TBD	TBD
		"	16. SA-9(c) External System Services	12/27/2024	P1	TBD	TBD	TBD
		"	17. SC-7(a) Boundary Protection	12/27/2024	P1	TBD	TBD	TBD
		"	18. SC-7(24)(b) Boundary Protection Personally Identifiable Information	12/27/2024	P1	TBD	TBD	TBD
		"	19. SC-18(b) Mobile Code	12/27/2024	P1	TBD	TBD	TBD
		"	20. SI-4 System Monitoring	12/27/2024	P1	TBD	TBD	TBD
		"	b. Establishing an ongoing frequency for monitoring and an ongoing frequency for assessment of control effectiveness;	12/27/2024	P1	TBD	TBD	TBD
		"	c. Ongoing control assessments in accordance with the continuous monitoring strategy;	12/27/2024	P1	TBD	TBD	TBD
		"	d. Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy;	12/27/2024	P1	TBD	TBD	TBD
		"	e. Correlation and analysis of information generated by control assessments and monitoring;	12/27/2024	P1	TBD	TBD	TBD
		"	f. Response actions to address results of the analysis of control assessment and monitoring information; and	12/27/2024	P1	TBD	TBD	TBD
		"	g. Reporting the security and privacy status of the system to organizational personnel with information security, privacy responsibilities, and system/network administrators annually, when security events/incidents occur, and when	12/27/2024	P1	TBD	TBD	TBD
	CA-7(1)	(1) CONTINUOUS MONITORING INDEPENDENT ASSESSMENT	Employ independent assessors or assessment teams to monitor the controls in the system on an ongoing basis.	12/27/2024	P1	TBD	TBD	TBD

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
	CA-7(4)	(4) CONTINUOUS MONITORING RISK MONITORING	Ensure risk monitoring is an integral part of the continuous monitoring strategy that includes the following:	12/27/2024	P1	TBD	TBD	TBD
		"	a. Effectiveness monitoring;	12/27/2024	P1	TBD	TBD	TBD
		"	b. Compliance monitoring; and	12/27/2024	P1	TBD	TBD	TBD
		"	c. Change monitoring.	12/27/2024	P1	TBD	TBD	TBD
	CA-9	INTERNAL SYSTEM CONNECTIONS	a. Authorize internal connections of components with the capability to process, store, or transmit CJI to the system;	Zero-cycle	P3	TBD	TBD	TBD
		"	b. Document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated;	Zero-cycle	P3	TBD	TBD	TBD
		"	c. Terminate internal system connections when no longer required or authorized; and	Zero-cycle	P3	TBD	TBD	TBD
		"	d. Review at least annually the continued need for each internal connection.	Zero-cycle	P3	TBD	TBD	TBD

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy: Configuration Management								
CM-1	CM-1	POLICY AND PROCEDURES	Develop, document, and disseminate to organizational personnel with configuration management responsibilities:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. Agency-level configuration management policy that:	Zero-cycle	P2	TBD	TBD	TBD
		"	(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Zero-cycle	P2	TBD	TBD	TBD
		"	(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and	Zero-cycle	P2	TBD	TBD	TBD
		"	2. Procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls;	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Designate organizational personnel with information security responsibilities to manage the development, documentation, and dissemination of the configuration management policy and procedures; and	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Review and update the current configuration management:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. Policy annually and following any hardware or software changes to systems which process, store, or transmit CJI; and	Zero-cycle	P2	TBD	TBD	TBD
		"	2. Procedures annually and following any hardware or software changes to systems which process, store, or transmit CJI.	Zero-cycle	P2	TBD	TBD	TBD
CM-2	CM-2	BASELINE CONFIGURATION	a. Develop, document, and maintain under configuration control, a current baseline configuration of the system;	10/1/2024	P1	TBD	TBD	TBD
		"	b. Develop, document, and maintain a current and complete topological drawing depicting the interconnectivity of the agency network to criminal justice information systems and services; and	Existing	P1	Agency	Both	Both
		"	c. Review and update the baseline configuration and topological drawing of the system:	Existing	P1	Agency	Both	Both
		"	1. At least annually;	Existing	P1	Agency	Both	Both
		"	2. When required due to security-relevant changes to the system and/or security incidents occur; and	Existing	P1	Agency	Both	Both
		"	3. When system components are installed or upgraded.	Existing	P1	Agency	Both	Both
CM-2(2)	CM-2(2)	(2) BASELINE CONFIGURATION AUTOMATION SUPPORT FOR ACCURACY AND CURRENCY	Maintain the currency, completeness, accuracy, and availability of the baseline configuration of the system using automated mechanisms such as configuration management tools, hardware, software, firmware inventory tools, and network management tools.	10/1/2024	P1	TBD	TBD	TBD
CM-2(3)	CM-2(3)	(3) BASELINE CONFIGURATION RETENTION OF PREVIOUS CONFIGURATIONS	Retain at least one (1) previous versions of baseline configurations of the system to support rollback.	10/1/2024	P1	TBD	TBD	TBD
CM-2(7)	CM-2(7)	(7) BASELINE CONFIGURATION CONFIGURE SYSTEMS AND COMPONENTS FOR HIGH-RISK AREAS	a. Issue devices (e.g., mobile devices) with CJISSECPOL compliant configurations to individuals traveling to locations that the organization deems to be of significant risk; and	10/1/2024	P1	TBD	TBD	TBD
		"	b. Apply the following controls to the systems or components when the individuals return from travel: examine the device for signs of physical tampering, purge and reimage disk drives and/or devices as required, and ensure all security controls are in place and functional	Existing	P1	Agency	Agency	Agency
CM-3	CM-3	CONFIGURATION CHANGE CONTROL	a. Determine and document the types of changes to the system that are configuration-controlled;	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses;	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Document configuration change decisions associated with the system:	Zero-cycle	P2	TBD	TBD	TBD

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CM-3	CM-3	CONFIGURATION CHANGE CONTROL (continued)	d. Implement approved configuration-controlled changes to the system;	Zero-cycle	P2	TBD	TBD	TBD
		"	e. Retain records of configuration-controlled changes to the system for two (2) years;	Zero-cycle	P2	TBD	TBD	TBD
		"	f. Monitor and review activities associated with configuration-controlled changes to the system; and	Zero-cycle	P2	TBD	TBD	TBD
		"	g. Coordinate and provide oversight for configuration change control activities through personnel with configuration management responsibilities, a Configuration Control Board, or Change Advisory Board that convenes regularly or when hardware or software changes (i.e., updates, upgrades, replacements, etc.) to the information system are required.	Zero-cycle	P2	TBD	TBD	TBD
CM-3(2)	CM-3(2)	(2) CONFIGURATION CHANGE CONTROL TESTING, VALIDATION, AND DOCUMENTATION OF CHANGES	Test, validate, and document changes to the system before finalizing the implementation of the changes.	Zero-cycle	P2	TBD	TBD	TBD
CM-3(4)	CM-3(4)	(4) CONFIGURATION CHANGE CONTROL SECURITY AND PRIVACY REPRESENTATIVES	Require organizational personnel with information security and privacy responsibilities to be members of the Configuration Control Board or Change Advisory Board.	Zero-cycle	P2	TBD	TBD	TBD
CM-4	CM-4	IMPACT ANALYSES	Analyze changes to the system to determine potential security and privacy impacts prior to change implementation.	Zero-cycle	P3	TBD	TBD	TBD
CM-4(2)	CM-4(2)	(2) IMPACT ANALYSES VERIFICATION OF CONTROLS	After system changes, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security and privacy requirements for the system.	Zero-cycle	P3	TBD	TBD	TBD
CM-5	CM-5	ACCESS RESTRICTIONS FOR CHANGE	Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.	Existing	P1	Agency	Both	Both
CM-6	CM-6	CONFIGURATION SETTINGS	a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using established best practices and guidelines such as Defense Information Systems Agency (DISA) Secure Technical Implementation Guidelines (STIGs), Center for Internet Security (CIS) Benchmarks, or Federal Information Processing Standards;	10/1/2024	P1	TBD	TBD	TBD
		"	b. Implement the configuration settings;	10/1/2024	P1	TBD	TBD	TBD
		"	c. Identify, document, and approve any deviations from established configuration settings for system components that store, process, or transmit CJI based on operational requirements; and	10/1/2024	P1	TBD	TBD	TBD
		"	d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.	10/1/2024	P1	TBD	TBD	TBD
CM-7	CM-7	LEAST FUNCTIONALITY	a. Configure the system to provide only essential capabilities to meet operational requirements; and	10/1/2024	P1	TBD	TBD	TBD
		"	b. Prohibit or restrict the use of specified functions, ports, protocols, software, and/or services: which are not required.	Existing	P1	Agency	Both	Both
CM-7(1)	CM-7(1)	(1) LEAST FUNCTIONALITY PERIODIC REVIEW	a. Review the system annually, as the system changes, or incidents occur to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services; and	Existing	P1	Agency	Both	Both
		"	b. Disable or remove functions, ports, protocols, software, and/or services within the system deemed to be unnecessary and/or unsecure.	10/1/2024	P1	TBD	TBD	TBD
CM-7(2)	CM-7(2)	(2) LEAST FUNCTIONALITY PREVENT PROGRAM EXECUTION	Prevent program execution in accordance with rules of behavior and/or rules authorizing the terms and conditions of software program usage.	10/1/2024	P1	TBD	TBD	TBD

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CM-7(5)	CM-7(5)	(5) LEAST FUNCTIONALITY AUTHORIZED SOFTWARE — ALLOW-BY-EXCEPTION	a. Identify software programs authorized to execute on the system;	10/1/2024	P1	TBD	TBD	TBD
		"	b. Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system; and	10/1/2024	P1	TBD	TBD	TBD
		"	c. Review and update the list of authorized software programs annually.	10/1/2024	P1	TBD	TBD	TBD
CM-8	CM-8	SYSTEM COMPONENT INVENTORY	a. Develop and document an inventory of system components that:	10/1/2024	P1	TBD	TBD	TBD
		"	1. Accurately reflects the system;	10/1/2024	P1	TBD	TBD	TBD
		"	2. Includes all components within the system;	10/1/2024	P1	TBD	TBD	TBD
		"	3. Does not include duplicate accounting of components or components assigned to any other system;	10/1/2024	P1	TBD	TBD	TBD
		"	4. Is at the level of granularity deemed necessary for tracking and reporting; and	10/1/2024	P1	TBD	TBD	TBD
		"	5. Includes the following minimum information to achieve system component accountability: date of installation, model, serial number, manufacturer, supplier information, component type, software owner, software version number, software license information, and hardware and physical location; and	10/1/2024	P1	TBD	TBD	TBD
		"	b. Review and update the system component inventory annually.	10/1/2024	P1	TBD	TBD	TBD
CM-8(1)	CM-8(1)	(1) SYSTEM COMPONENT INVENTORY UPDATES DURING INSTALLATION AND REMOVAL	Update the inventory of system components as part of component installations, removals, and system updates.	10/1/2024	P1	TBD	TBD	TBD
CM-8(3)	CM-8(3)	(3) SYSTEM COMPONENT INVENTORY AUTOMATED UNAUTHORIZED COMPONENT DETECTION	a. Detect the presence of unauthorized hardware, software, and firmware components within the system using automated mechanisms continuously or at least weekly; and	10/1/2024	P1	TBD	TBD	TBD
		"	b. Take the following actions when unauthorized components are detected: disable or isolate the unauthorized components and notify organizational personnel with security responsibilities.	10/1/2024	P1	TBD	TBD	TBD
CM-9	CM-9	CONFIGURATION MANAGEMENT PLAN	Develop, document, and implement a configuration management plan for the system that:	Zero-cycle	P2	TBD	TBD	TBD
		"	a. Addresses roles, responsibilities, and configuration management processes and procedures;	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Defines the configuration items for the system and places the configuration items under configuration management;	Zero-cycle	P2	TBD	TBD	TBD
		"	d. Is reviewed and approved by organizational personnel with information security responsibilities and organizational personnel with configuration management responsibilities; and	Zero-cycle	P2	TBD	TBD	TBD
		"	e. Protects the configuration management plan from unauthorized disclosure and modification.	Zero-cycle	P2	TBD	TBD	TBD
CM-10	CM-10	SOFTWARE USAGE RESTRICTIONS	a. Use software and associated documentation in accordance with contract agreements and copyright laws;	Zero-cycle	P3	TBD	TBD	TBD
		"	b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and	Zero-cycle	P3	TBD	TBD	TBD
		"	c. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.	Zero-cycle	P3	TBD	TBD	TBD

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CM-11	CM-11	USER-INSTALLED SOFTWARE	a. Establish agency-level policies governing the installation of software by users;	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Enforce software installation policies through automated methods; and	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Monitor policy compliance through automated methods at least weekly.	Zero-cycle	P2	TBD	TBD	TBD
CM-12	CM-12	INFORMATION LOCATION	a. Identify and document the location of CJI and the specific system components on which the information is processed, stored, or transmitted;	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Identify and document the users who have access to the system and system components where the information is processed and stored; and	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Document changes to the location (i.e., system or system components) where the information is processed and stored.	Zero-cycle	P2	TBD	TBD	TBD
CM-12(1)	CM-12(1)	(1) INFORMATION LOCATION AUTOMATED TOOLS TO SUPPORT INFORMATION LOCATION	Use automated tools to identify CJI on software and hardware system components to ensure controls are in place to protect organizational information and individual privacy.	Zero-cycle	P2	TBD	TBD	TBD

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy: Contingency Planning (CP)								
CP-1	CP-1	POLICY AND PROCEDURES	a. Develop, document, and disseminate to organizational personnel with contingency planning responsibilities:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. Agency-level contingency planning policy that:	Zero-cycle	P2	TBD	TBD	TBD
		"	(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Zero-cycle	P2	TBD	TBD	TBD
		"	(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and	Zero-cycle	P2	TBD	TBD	TBD
		"	2. Procedures to facilitate the implementation of the contingency planning policy and the associated contingency planning controls;	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Designate organizational personnel with information security responsibilities to manage the development, documentation, and dissemination of the contingency planning policy and procedures; and	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Review and update the current contingency planning:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. Policy annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI, or training simulations or exercises; and	Zero-cycle	P2	TBD	TBD	TBD
		"	2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI, or training simulations or exercises.	Zero-cycle	P2	TBD	TBD	TBD
CP-2	CP-2	CONTINGENCY PLAN	a. Develop a contingency plan for the system that:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. Identifies essential mission and business functions and associated contingency requirements;	Zero-cycle	P2	TBD	TBD	TBD
		"	2. Provides recovery objectives, restoration priorities, and metrics;	Zero-cycle	P2	TBD	TBD	TBD
		"	3. Addresses contingency roles, responsibilities, assigned individuals with contact information;	Zero-cycle	P2	TBD	TBD	TBD
		"	4. Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure;	Zero-cycle	P2	TBD	TBD	TBD
		"	5. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented;	Zero-cycle	P2	TBD	TBD	TBD
		"	6. Addresses the sharing of contingency information; and	Zero-cycle	P2	TBD	TBD	TBD
		"	7. Is reviewed and approved by agency head or their designee;	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Distribute copies of the contingency plan to organizational personnel with contingency planning or incident response duties;	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Coordinate contingency planning activities with incident handling activities;	Zero-cycle	P2	TBD	TBD	TBD
		"	d. Review the contingency plan for the system annually;	Zero-cycle	P2	TBD	TBD	TBD
		"	e. Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;	Zero-cycle	P2	TBD	TBD	TBD
		"	f. Communicate contingency plan changes to organizational personnel with contingency planning or incident response duties;	Zero-cycle	P2	TBD	TBD	TBD
		"	g. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; and	Zero-cycle	P2	TBD	TBD	TBD
		"	h. Protect the contingency plan from unauthorized disclosure and modification.	Zero-cycle	P2	TBD	TBD	TBD
CP-2 (1)	CP-2 (1)	(1) CONTINGENCY PLAN COORDINATE WITH RELATED PLANS	Coordinate contingency plan development with organizational elements responsible for related plans.	Zero-cycle	P2	TBD	TBD	TBD
CP-2 (3)	CP-2 (3)	(3) CONTINGENCY PLAN RESUME MISSION AND BUSINESS FUNCTIONS	Plan for the resumption of essential mission and business functions within twenty-four (24) hours of contingency plan activation.	Zero-cycle	P2	TBD	TBD	TBD

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CP-2 (8)	CP-2 (8)	(8) CONTINGENCY PLAN IDENTIFY CRITICAL ASSETS	Identify critical system assets supporting essential mission and business functions.	Zero-cycle	P2	TBD	TBD	TBD
CP-3	CP-3	CONTINGENCY TRAINING	a. Provide contingency training to system users consistent with assigned roles and responsibilities:	Zero-cycle	P3	TBD	TBD	TBD
		"	1. Within thirty (30) days of assuming a contingency role or responsibility;	Zero-cycle	P3	TBD	TBD	TBD
		"	2. When required by system changes; and	Zero-cycle	P3	TBD	TBD	TBD
		"	3. Annually thereafter; and	Zero-cycle	P3	TBD	TBD	TBD
		"	b. Review and update contingency training content annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI, or training simulations or exercises.	Zero-cycle	P3	TBD	TBD	TBD
CP-4	CP-4	CONTINGENCY PLAN TESTING	a. Test the contingency plan for the system annually using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: checklists, walk-through and tabletop exercises, simulations (parallel or full interrupt), or comprehensive exercises.	Zero-cycle	P3	TBD	TBD	TBD
		"	b. Review the contingency plan test results; and	Zero-cycle	P3	TBD	TBD	TBD
		"	c. Initiate corrective actions, if needed.	Zero-cycle	P3	TBD	TBD	TBD
CP-4 (1)	CP-4 (1)	(1) CONTINGENCY PLAN TESTING COORDINATE WITH RELATED PLANS	Coordinate contingency plan testing with organizational elements responsible for related plans.	Zero-cycle	P3	TBD	TBD	TBD
CP-6	CP-6	ALTERNATE STORAGE SITE	a. Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information; and	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Ensure that the alternate storage site provides controls equivalent to that of the primary site.	Zero-cycle	P2	TBD	TBD	TBD
CP-6 (1)	CP-6 (1)	(1) ALTERNATE STORAGE SITE SEPARATION FROM PRIMARY SITE	Identify an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats.	Zero-cycle	P2	TBD	TBD	TBD
CP-6 (3)	CP-6 (3)	(3) ALTERNATE STORAGE SITE ACCESSIBILITY	Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.	Zero-cycle	P2	TBD	TBD	TBD
CP-7	CP-7	ALTERNATE PROCESSING SITE	a. Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of operations for essential mission and business functions within the time period defined in the system contingency plan(s) when the primary processing capabilities are unavailable;	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Make available at the alternate processing site, the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery to the site within the organization-defined time period for transfer and resumption; and	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Provide controls at the alternate processing site that are equivalent to those at the primary site.	Zero-cycle	P2	TBD	TBD	TBD
CP-7 (1)	CP-7 (1)	(1) ALTERNATE PROCESSING SITE SEPARATION FROM PRIMARY SITE	Identify an alternate processing site that is sufficiently separated from the primary processing site to reduce susceptibility to the same threats.	Zero-cycle	P2	TBD	TBD	TBD
CP-7 (2)	CP-7 (2)	(2) ALTERNATE PROCESSING SITE ACCESSIBILITY	Identify potential accessibility problems to alternate processing sites in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.	Zero-cycle	P2	TBD	TBD	TBD
CP-7 (3)	CP-7 (3)	(3) ALTERNATE PROCESSING SITE PRIORITY OF SERVICE	Develop alternate processing site agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives).	Zero-cycle	P2	TBD	TBD	TBD

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CP-8	CP-8	TELECOMMUNICATIONS SERVICES	Establish alternate telecommunications services, including necessary agreements to permit the resumption of system operations for essential mission and business functions within the time period as defined in the system contingency plan(s) when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.	Zero-cycle	P2	TBD	TBD	TBD
CP-8 (1)	CP-8 (1)	(1) TELECOMMUNICATIONS SERVICES PRIORITY OF SERVICE PROVISIONS	(a) Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives); and	Zero-cycle	P2	TBD	TBD	TBD
		"	(b) Request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness if the primary and/or alternate telecommunications services are provided by a common carrier.	Zero-cycle	P2	TBD	TBD	TBD
CP-8 (2)	CP-8 (2)	(2) TELECOMMUNICATIONS SERVICES SINGLE POINTS OF FAILURE	Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.	Zero-cycle	P2	TBD	TBD	TBD
CP-9	CP-9	SYSTEM BACKUP	a. Conduct backups of user-level information contained in operational systems for essential business functions as required by the contingency plans;	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Conduct backups of system-level information contained in the system as required by the contingency plans;	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Conduct backups of system documentation, including security- and privacy-related documentation as required by the contingency plans; and	Zero-cycle	P2	TBD	TBD	TBD
		"	d. Protect the confidentiality, integrity, and availability of backup information.	Zero-cycle	P2	TBD	TBD	TBD
CP-9 (1)	CP-9 (1)	(1) SYSTEM BACKUP TESTING FOR RELIABILITY AND INTEGRITY	Test backup information as required by the contingency plans to verify media reliability and information integrity.	Zero-cycle	P2	TBD	TBD	TBD
CP-9 (8)	CP-9 (8)	(8) SYSTEM BACKUP CRYPTOGRAPHIC PROTECTION	Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of CJI.	Zero-cycle	P2	TBD	TBD	TBD
CP-10	CP-10	SYSTEM RECOVERY AND RECONSTITUTION	Provide for the recovery and reconstitution of the system to a known state within the timeframe as required by the contingency plans after a disruption, compromise, or failure.	Zero-cycle	P2	TBD	TBD	TBD
CP-10 (2)	CP-10 (2)	(2) SYSTEM RECOVERY AND RECONSTITUTION TRANSACTION RECOVERY	Implement transaction recovery for systems that are transaction-based.	Zero-cycle	P2	TBD	TBD	TBD

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy: Identification and Authentication (IA)								
5.6: IA-0	IA-0	Use of Originating Agency Identifiers in Transactions and Information Exchanges	An FBI authorized originating agency identifier (ORI) shall be used in each transaction on CJIS systems in order to identify the sending agency and to ensure the proper level of access for each transaction.	Existing	Existing	Agency	Agency	Agency
		"	The original identifier between the requesting agency and the CSA/SIB/Channeler shall be the ORI, and other agency identifiers, such as user identification or personal identifier, an access device mnemonic, or the Internet Protocol (IP) address.	Existing	Existing	Agency	Agency	Agency
		"	Because the agency performing the transaction may not necessarily be the same as the agency requesting the transaction, the CSA/SIB/Channeler shall ensure that the ORI for each transaction can be traced, via audit trail, to the specific agency which is requesting the transaction.	Existing	Existing	Agency	Agency	Agency
		"	Agencies assigned a limited access ORI shall not use the full access ORI of another agency to conduct an inquiry transaction.	Existing	Existing	Agency	Agency	Agency
5.6: IA-1	IA-1	Policy and Procedures	a. Develop, document, and disseminate to authorized personnel:	Zero-cycle	P2	Agency	Agency	Agency
		"	1. Agency/Entity identification and authentication policy that:	Zero-cycle	P2	Agency	Agency	Agency
		"	(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Zero-cycle	P2	Agency	Agency	Agency
		"	(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and	Zero-cycle	P2	Agency	Agency	Agency
		"	2. Procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls;	Zero-cycle	P2	Agency	Agency	Agency
		"	b. Designate an individual with security responsibilities to manage the development, documentation, and dissemination of the identification and authentication policy and procedures; and	Zero-cycle	P2	Agency	Agency	Agency
		"	c. Review and update the current identification and authentication:	Zero-cycle	P2	Agency	Agency	Agency
		"	1. Policy annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI; and	Zero-cycle	P2	Agency	Agency	Agency
		"	2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.	Zero-cycle	P2	Agency	Agency	Agency
5.6: IA-2	IA-2	Identification and Authentication (Organizational Users)	Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.	Existing	P1	Agency	Agency	Agency
5.6: IA-2 (1)	IA-2 (1)	Identification and Authentication (Organizational Users) Multi-Factor Authentication to Privileged Accounts	Implement multi-factor authentication for access to privileged accounts.	10/1/2024	P1	Agency	Both	Both
5.6: IA-2 (2)	IA-2 (2)	Identification and Authentication (Organizational Users) Multi-Factor Authentication to Non-Privileged Accounts	Implement multi-factor authentication for access to non-privileged accounts.	10/1/2024	P1	Agency	Both	Both
5.6: IA-2 (8)	IA-2 (8)	Identification and Authentication (Organizational Users) Access to Accounts - Replay Resistant	Implement replay-resistant authentication mechanisms for access to privileged and non-privileged accounts.	10/1/2024	P1	Agency	Both	Both
5.6: IA-2 (12)	IA-2 (12)	Identification and Authentication (Organizational Users) Acceptance of PIV Credentials	Accept and electronically verify Personal Identity Verification-compliant credentials.	10/1/2024	P1	Agency	Both	Both
5.6: IA-3	IA-3	Device Identification and Authentication	Uniquely identify and authenticate agency devices before establishing all remote and network connections. In the instance of local connection, the device must be approved by the agency and the device must be identified and authenticated prior to connection to an agency asset.	Zero-cycle	P2	Agency	Both	Both

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
5.6: IA-4	IA-4	Identifier Management	Manage system identifiers by:	Existing	P2	Agency	Both	Both
		"	a. Receiving authorization from organizational personnel with identifier management responsibilities to assign an individual, group, role, service, or device identifier;	Existing	P2	Agency	Both	Both
		"	b. Selecting an identifier that identifies an individual, group, role, service, or device;	Existing	P2	Agency	Both	Both
		"	c. Assigning the identifier to the intended individual, group, role, service, or device; and	Existing	P2	Agency	Both	Both
		"	d. Preventing reuse of identifiers for one (1) year.	Zero-cycle	P2	Agency	Both	Both
5.6: IA-4 (4)	IA-4 (4)	Identifier Management Identify User Status	Manage individual identifiers by uniquely identifying each individual as agency or non-agency.	Zero-cycle	P2	Agency	Both	Both
5.6: IA-5	IA-5	Authenticator Management	Manage system authenticators by:	Existing	P1	Agency	Both	Both
		"	a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator;	Existing	P1	Agency	Both	Both
		"	b. Establishing initial authenticator content for any authenticators issued by the organization;	Existing	P1	Agency	Both	Both
		"	c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;	10/1/2024	P1	Agency	Both	Both
		"	d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators;	Existing	P1	Agency	Both	Both
		"	e. Changing default authenticators prior to first use;	Existing	P1	Agency	Both	Both
		"	f. Changing or refreshing authenticators annually or when there is evidence of authenticator compromise; changing or refreshing all other authenticator types as they expire or when there is evidence of authenticator compromise;	Existing	P1	Agency	Both	Both
		"	g. Protecting authenticator content from unauthorized disclosure and modification;	Existing	P1	Agency	Both	Both
		"	h. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and	10/1/2024	P1	Agency	Both	Both
		"	i. Changing authenticators for group or role accounts when membership to those accounts changes.	10/1/2024	P1	Agency	Both	Both
		"	j. All credential service providers (CSPs) authenticating claimants at Authenticator Assurance Level 2 (AAL2) SHALL be assessed on the following criteria:	10/1/2024	P1			
		"	(1) Authentication SHALL occur by the use of either a multi-factor authenticator or a combination of two single-factor authenticators.	10/1/2024	P1	Agency	Both	Both
		"	(2) If the multi-factor authentication process uses a combination of two single-factor authenticators, then it SHALL include a Memorized Secret authenticator and a possession-based authenticator. (NIST 800-63B, Section	10/1/2024	P1	Agency	Both	Both
		"	(3) Cryptographic authenticators used at AAL2 SHALL use approved cryptography.	10/1/2024	P1	Agency	Both	Both
		"	(4) At least one authenticator used at AAL2 SHALL be replay resistant.	10/1/2024	P1	Agency	Both	Both
		"	(5) Communication between the claimant and verifier SHALL be via an authenticated protected channel.	10/1/2024	P1	Agency	Both	Both
		"	(6) Verifiers operated by government agencies at AAL2 SHALL be validated to meet the requirements of FIPS 140 Level 1.	10/1/2024	P1	Agency	Both	Both
		"	(7) Authenticators procured by government agencies SHALL be validated to meet the requirements of FIPS 140 Level 1.	10/1/2024	P1	Agency	Both	Both

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
5.6: IA-5	IA-5	Authenticator Management (continued)	(8) If a device such as a smartphone is used in the authentication process, then the unlocking of that device (typically done using a PIN or biometric) SHALL NOT be considered one of the authentication factors.	10/1/2024	P1	Agency	Both	Both
		"	(9) If a biometric factor is used in authentication at AAL2, then the performance requirements stated in IA-5 m Biometric Requirements SHALL be	10/1/2024	P1	Agency	Both	Both
		"	(10) Reauthentication of the subscriber SHALL be repeated at least once per 12 hours during an extended usage session.	10/1/2024	P1	Agency	Both	Both
		"	(11) Reauthentication of the subscriber SHALL be repeated following any period of inactivity lasting 30 minutes or longer.	10/1/2024	P1	Agency	Both	Both
		"	(12) The CSP SHALL employ appropriately tailored security controls from the moderate baseline of security controls defined in the CJIS Security Policy.	10/1/2024	P1	Agency	Both	Both
		"	The CSP SHALL ensure that the minimum assurance-related controls for moderate-impact systems are satisfied.	10/1/2024	P1	Agency	Both	Both
		"	(13) The CSP SHALL comply with records retention policies in accordance with applicable laws and regulations.	10/1/2024	P1	Agency	Both	Both
		"	(14) If the CSP opts to retain records in the absence of any mandatory requirements, then the CSP SHALL conduct a risk management process, including assessments of privacy and security risks to determine how long records should be retained and SHALL inform subscribers of that retention policy.	10/1/2024	P1	Agency	Both	Both
		"	k. Privacy requirements that apply to all CSPs, verifiers, and RPs.	10/1/2024	P1			
		"	(1) The CSP SHALL employ appropriately tailored privacy controls from the CJIS Security Policy.	10/1/2024	P1	Agency	Both	Both
		"	(2) If the CSP processes attributes for purposes other than identity proofing, authentication, or attribute assertions (collectively "identity service"), related fraud mitigation, or to comply with law or legal process, then the CSP SHALL implement measures to maintain predictability and manageability commensurate with the associated privacy risk.	10/1/2024	P1	Agency	Both	Both
		"	l. General requirements applicable to AAL2 authentication process.	10/1/2024	P1			
		"	(1) CSPs SHALL provide subscriber instructions on how to appropriately protect a physical authenticator against theft or loss.	10/1/2024	P1	Agency	Both	Both
		"	(2) The CSP SHALL provide a mechanism to revoke or suspend the authenticator immediately upon notification from subscriber that loss or theft of the authenticator is suspected.	10/1/2024	P1	Agency	Both	Both
		"	(3) If required by the authenticator type descriptions in IA-5(1), then the verifier SHALL implement controls to protect against online guessing attacks.	10/1/2024	P1	Agency	Both	Both
		"	(4) If required by the authenticator type descriptions in IA-5(1) and the description of a given authenticator does not specify otherwise, then the verifier SHALL limit consecutive failed authentication attempts on a single account to no more than 100.	10/1/2024	P1	Agency	Both	Both
		"	(5) If signed attestations are used, then they SHALL be signed using a digital signature that provides at least the minimum security strength specified in the latest revision of 112 bits as of the date of this publication.	10/1/2024	P1	Agency	Both	Both
		"	(6) If the verifier and CSP are separate entities (as shown by the dotted line in Figure 8 Digital Identity Model), then communications between the verifier and CSP SHALL occur through a mutually-authenticated secure channel (such as a client-authenticated TLS connection).	10/1/2024	P1	Agency	Both	Both
		"	(7) If the CSP provides the subscriber with a means to report loss, theft, or damage to an authenticator using a backup or alternate authenticator, then that authenticator SHALL be either a memorized secret or a physical authenticator.	10/1/2024	P1	Agency	Both	Both

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
5.6: IA-5	IA-5	Authenticator Management (continued)	(8) If the CSP chooses to verify an address of record (i.e., email, telephone, postal) and suspend authenticator(s) reported to have been compromised, then...The suspension SHALL be reversible if the subscriber successfully authenticates to the CSP using a valid (i.e., not suspended) authenticator and requests reactivation of an authenticator suspended in this manner.	10/1/2024	P1	Agency	Both	Both
		"	(9) If and when an authenticator expires, it SHALL NOT be usable for authentication.	10/1/2024	P1	Agency	Both	Both
		"	(10) The CSP SHALL have a documented process to require subscribers to surrender or report the loss of any physical authenticator containing attribute certificates signed by the CSP as soon as practical after expiration or receipt of a renewed authenticator.	10/1/2024	P1	Agency	Both	Both
		"	(11) CSPs SHALL revoke the binding of authenticators immediately upon notification when an online identity ceases to exist (e.g., subscriber's death, discovery of a fraudulent subscriber), when requested by the subscriber, or when the CSP determines that the subscriber no longer meets its eligibility requirements.	10/1/2024	P1	Agency	Both	Both
		"	(12) The CSP SHALL have a documented process to require subscribers to surrender or report the loss of any physical authenticator containing certified attributes signed by the CSP within five (5) days after revocation or termination takes place.	10/1/2024	P1	Agency	Both	Both
		"	m. Biometric Requirements	10/1/2024	P1			
		"	(1) Biometrics SHALL be used only as part of multi-factor authentication with a physical authenticator (something you have).	10/1/2024	P1	Agency	Both	Both
		"	(2) An authenticated protected channel between sensor (or an endpoint containing a sensor that resists sensor replacement) and verifier SHALL be established.	10/1/2024	P1	Agency	Both	Both
		"	(3) The sensor or endpoint SHALL be authenticated prior to capturing the biometric sample from the claimant.	10/1/2024	P1	Agency	Both	Both
		"	(4) The biometric system SHALL operate with an FMR [ISO/IEC 2382-37] of 1 in 1000 or better. This FMR SHALL be achieved under conditions of a conformant attack (i.e., zero-effort impostor attempt) as defined in [ISO/IEC 30107-1].	10/1/2024	P1	Agency	Both	Both
		"	(5) The biometric system SHALL allow no more than 5 consecutive failed authentication attempts or 10 consecutive failed attempts if PAD demonstrating at least 90% resistance to presentation attacks is implemented.	10/1/2024	P1	Agency	Both	Both
		"	(6) Once the limit on authentication failures has been reached, the biometric authenticator SHALL either:	10/1/2024	P1	Agency	Both	Both
		"	i. Impose a delay of at least 30 seconds before the next attempt, increasing exponentially with each successive attempt, or	10/1/2024	P1	Agency	Both	Both
		"	ii. disable the biometric user authentication and offer another factor (e.g., a different biometric modality or a PIN/Passcode if it is not already a required factor) if such an alternative method is already available.	10/1/2024	P1	Agency	Both	Both
		"	(7) The verifier SHALL make a determination of sensor and endpoint performance, integrity, and authenticity.	10/1/2024	P1	Agency	Both	Both
		"	(8) If biometric comparison is performed centrally, then use of the biometric as an authentication factor SHALL be limited to one or more specific devices that are identified using approved cryptography.	10/1/2024	P1	Agency	Both	Both
		"	(9) If biometric comparison is performed centrally, then a separate key SHALL be used for identifying the device.	10/1/2024	P1	Agency	Both	Both

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
5.6: IA-5	IA-5	Authenticator Management (continued)	(10) If biometric comparison is performed centrally, then biometric revocation, referred to as biometric template protection in ISO/IEC 24745, SHALL be implemented.	10/1/2024	P1	Agency	Both	Both
		"	(11) If biometric comparison is performed centrally, all transmission of biometrics SHALL be over the authenticated protected channel.	10/1/2024	P1	Agency	Both	Both
		"	(12) Biometric samples and any biometric data derived from the biometric sample such as a probe produced through signal processing SHALL be zeroized immediately after any training or research data has been derived	10/1/2024	P1	Agency	Both	Both
		"	n. Authenticator binding refers to the establishment of an association between a specific authenticator and a subscriber's account, enabling the authenticator to be used — possibly in conjunction with other authenticators — to authenticate for that account.	10/1/2024	P1			
		"	(1) Authenticators SHALL be bound to subscriber accounts by either issuance by the CSP as part of enrollment or associating a subscriber-provided authenticator that is acceptable to the CSP.	10/1/2024	P1	Agency	Both	Both
		"	(2) Throughout the digital identity lifecycle, CSPs SHALL maintain a record of all authenticators that are or have been associated with each identity.	10/1/2024	P1	Agency	Both	Both
		"	(3) The CSP or verifier SHALL maintain the information required for throttling authentication attempts.	10/1/2024	P1	Agency	Both	Both
		"	(4) The CSP SHALL also verify the type of user-provided authenticator so verifiers can determine compliance with requirements at each AAL.	10/1/2024	P1	Agency	Both	Both
		"	(5) The record created by the CSP SHALL contain the date and time the authenticator was bound to the account.	10/1/2024	P1	Agency	Both	Both
		"	(6) When any new authenticator is bound to a subscriber account, the CSP SHALL ensure that the binding protocol and the protocol for provisioning the associated key(s) are done at AAL2.	10/1/2024	P1	Agency	Both	Both
		"	(7) Protocols for key provisioning SHALL use authenticated protected channels or be performed in person to protect against man-in-the- middle attacks.	10/1/2024	P1	Agency	Both	Both
		"	(8) Binding of multi-factor authenticators SHALL require multi-factor authentication (or equivalent) at identity proofing.	10/1/2024	P1	Agency	Both	Both
		"	(9) At enrollment, the CSP SHALL bind at least one, and SHOULD bind at least two, physical (something you have) authenticators to the subscriber's online identity, in addition to a memorized secret or one or more biometrics.	10/1/2024	P1	Agency	Both	Both
		"	(10) At enrollment, authenticators at AAL2 and IAL2 SHALL be bound to the account.	10/1/2024	P1	Agency	Both	Both
		"	(11) If the subscriber is authenticated at AAL1, then the CSP SHALL NOT expose personal information, even if self-asserted, to the subscriber.	10/1/2024	P1	Agency	Both	Both
		"	(12) If enrollment and binding are being done remotely and cannot be completed in a single electronic transaction, then the applicant SHALL identify themselves in each new binding transaction by presenting a temporary secret which was either established during a prior transaction, or sent to the applicant's phone number, email address, or postal address of record.	10/1/2024	P1	Agency	Both	Both
		"	(13) If enrollment and binding are being done remotely and cannot be completed in a single electronic transaction, then long-term authenticator secrets are delivered to the applicant within a protected session.	10/1/2024	P1	Agency	Both	Both
		"	(14) If enrollment and binding are being done in person and cannot be completed in a single physical encounter, the applicant SHALL identify themselves in person by either using a secret as described in IA-5 n (12) above, or through use of a biometric that was recorded during a prior encounter.	10/1/2024	P1	Agency	Both	Both

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
5.6: IA-5	IA-5	Authenticator Management (continued)	(15) If enrollment and binding are being done in person and cannot be completed in a single physical encounter, temporary secrets SHALL NOT be reused.	10/1/2024	P1	Agency	Both	Both
		"	(16) If enrollment and binding are being done in person and cannot be completed in a single physical encounter and the CSP issues long-term authenticator secrets during a physical transaction, they SHALL be loaded locally onto a physical device that is issued in person to the applicant or delivered in a manner that confirms the address of record.	10/1/2024	P1	Agency	Both	Both
		"	(17) Before adding a new authenticator to a subscriber's account, the CSP SHALL first require the subscriber to authenticate at AAL2 (or a higher AAL) at which the new authenticator will be used.	10/1/2024	P1	Agency	Both	Both
		"	(18) If the subscriber's account has only one authentication factor bound to it, the CSP SHALL require the subscriber to authenticate at AAL1 in order to bind an additional authenticator of a different authentication factor.	10/1/2024	P1	Agency	Both	Both
		"	(19) If a subscriber loses all authenticators of a factor necessary to complete multi-factor authentication and has been identity proofed at IAL2, that subscriber SHALL repeat the identity proofing process described in IA-12.	10/1/2024	P1	Agency	Both	Both
		"	(20) If a subscriber loses all authenticators of a factor necessary to complete multi-factor authentication and has been identity proofed at IAL2 or IAL3, the CSP SHALL require the claimant to authenticate using an authenticator of the remaining factor, if any, to confirm binding to the existing identity.	10/1/2024	P1	Agency	Both	Both
		"	(21) If the CSP opts to allow binding of a new memorized secret with the use of two physical authenticators, then it requires entry of a confirmation code sent to an address of record.	10/1/2024	P1	Agency	Both	Both
		"	(22) If the CSP opts to allow binding of a new memorized secret with the use of two physical authenticators, then the confirmation code SHALL consist of at least 6 random alphanumeric characters generated by an approved random bit generator [SP 800-90Ar1].	10/1/2024	P1	Agency	Both	Both
		"	(23) If the CSP opts to allow binding of a new memorized secret with the use of two physical authenticators, then the confirmation code SHALL be valid for a maximum of 7 days but MAY be made valid up to 21 days via an exception process to accommodate addresses outside the direct reach of the U.S. Postal Service. Confirmation codes sent by means other than physical mail SHALL be valid for a maximum of 5 minutes.	10/1/2024	P1	Agency	Both	Both
		"	o. Session Management: The following requirements apply to applications where a session is maintained between the subscriber and relying party to allow multiple interactions without repeating the authentication event each time.	10/1/2024	P1			
		"	(1) Session Binding Requirements: A session occurs between the software that a subscriber is running — such as a browser, application, or operating system (i.e., the session subject) — and the RP or CSP that the subscriber is accessing (i.e., the session host).	10/1/2024	P1	Agency	Both	Both
		"	a. A session is maintained by a session secret which SHALL be shared between the subscriber's software and the service being accessed.	10/1/2024	P1	Agency	Both	Both
		"	b. The secret SHALL be presented directly by the subscriber's software or possession of the secret SHALL be proven using a cryptographic mechanism.	10/1/2024	P1	Agency	Both	Both
		"	c. The secret used for session binding SHALL be generated by the session host in direct response to an authentication event.	10/1/2024	P1	Agency	Both	Both
		"	d. A session SHALL NOT be considered at a higher AAL than the authentication event.	10/1/2024	P1	Agency	Both	Both

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
5.6: IA-5	IA-5	Authenticator Management (continued)	e. Secrets used for session binding SHALL be generated by the session host during an interaction, typically immediately following authentication.	10/1/2024	P1	Agency	Both	Both
		"	f. Secrets used for session binding SHALL be generated by an approved random bit generator [SP 800-90Ar1].	10/1/2024	P1	Agency	Both	Both
		"	g. Secrets used for session binding SHALL contain at least 64 bits of entropy.	10/1/2024	P1	Agency	Both	Both
		"	h. Secrets used for session binding SHALL be erased or invalidated by the session subject when the subscriber logs out.	10/1/2024	P1	Agency	Both	Both
		"	i. Secrets used for session binding SHALL be sent to and received from the device using an authenticated protected channel.	10/1/2024	P1	Agency	Both	Both
		"	j. Secrets used for session binding SHALL time out and not be accepted after the times specified in IA-5 j (13) as appropriate for the AAL.	10/1/2024	P1	Agency	Both	Both
		"	k. Secrets used for session binding SHALL NOT be available to insecure communications between the host and subscriber's endpoint.	10/1/2024	P1	Agency	Both	Both
		"	l. Authenticated sessions SHALL NOT fall back to an insecure transport, such as from https to http, following authentication.	10/1/2024	P1	Agency	Both	Both
		"	m. URLs or POST content SHALL contain a session identifier that SHALL be verified by the RP to ensure that actions taken outside the session do not affect the protected session.	10/1/2024	P1	Agency	Both	Both
		"	n. Browser cookies SHALL be tagged to be accessible only on secure (HTTPS) sessions.	10/1/2024	P1	Agency	Both	Both
		"	o. Browser cookies SHALL be accessible to the minimum practical set of hostnames and paths.	10/1/2024	P1	Agency	Both	Both
		"	p. Expiration of browser cookies SHALL NOT be depended upon to enforce session timeouts.	10/1/2024	P1	Agency	Both	Both
		"	q. The presence of an OAuth access token SHALL NOT be interpreted by the RP as presence of the subscriber, in the absence of other signals.	10/1/2024	P1	Agency	Both	Both
		"	(2) Reauthentication Requirements	10/1/2024	P1			
		"	a. Continuity of authenticated sessions SHALL be based upon the possession of a session secret issued by the verifier at the time of authentication and optionally refreshed during the session.	10/1/2024	P1	Agency	Both	Both
		"	b. Session secrets SHALL be non-persistent, i.e., they SHALL NOT be retained across a restart of the associated application or a reboot of the host device.	10/1/2024	P1	Agency	Both	Both
		"	c. Periodic reauthentication of sessions (at least every 12 hours per session) SHALL be performed to confirm the continued presence of the subscriber at an authenticated session.	10/1/2024	P1	Agency	Both	Both
		"	d. A session SHALL NOT be extended past the guidelines in IA-5 o (2) a – j based on presentation of the session secret alone.	10/1/2024	P1	Agency	Both	Both
		"	e. Prior to session expiration, the reauthentication time limit SHALL be extended by prompting the subscriber for the authentication factor(s) of a memorized secret or biometric.	10/1/2024	P1	Agency	Both	Both
		"	f. If federated authentication is being used, then since the CSP and RP often employ separate session management technologies, there SHALL NOT be any assumption of correlation between these sessions.	10/1/2024	P1	Agency	Both	Both
		"	g. An RP requiring reauthentication through a federation protocol SHALL — if possible within the protocol — specify the maximum (see IA-5 j (10)) acceptable authentication age to the CSP.	10/1/2024	P1	Agency	Both	Both

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
5.6: IA-5	IA-5	Authenticator Management (continued)	h. If federated authentication is being used and an RP has specific authentication age (see IA-5 j (10)) requirements that it has communicated to the CSP, then the CSP SHALL reauthenticate the subscriber if they have not been authenticated within that time period.	10/1/2024	P1	Agency	Both	Both
		"	i. If federated authentication is being used, the CSP SHALL communicate the authentication event time to the RP to allow the RP to decide if the assertion is sufficient for reauthentication and to determine the time for the next reauthentication event.	10/1/2024	P1	Agency	Both	Both
5.6: IA-5 (1)	IA-5 (1)	Authenticator Management Authenticator Types	(a) Memorized Secret Authenticators and Verifiers:	Existing	P1			
		"	(1) 1.Maintain a list of commonly-used, expected, or compromised passwords via API or download from a third party. Update the list quarterly and when organizational passwords are suspected to have been compromised directly or indirectly. Compare current memorized secrets against the list quarterly;	Existing	P1	Agency	Both	Both
		"	(2) Require immediate selection of a new password upon account recovery;	10/1/2024	P1	Agency	Both	Both
		"	(3) Allow user selection of long passwords and passphrases, including spaces and all printable characters;	10/1/2024	P1	Agency	Both	Both
		"	(4) Employ automated tools to assist the user in selecting strong password authenticators;	10/1/2024	P1	Agency	Both	Both
		"	(5) If chosen by the subscriber, memorized secrets SHALL be at least 8 characters in length.	Existing	P1	Agency	Both	Both
		"	(6) If chosen by the CSP or verifier using an approved random number generator, memorized secrets SHALL be at least 6 characters in length.	10/1/2024	P1	Agency	Both	Both
		"	(7) Truncation of the secret SHALL NOT be performed.	10/1/2024	P1	Agency	Both	Both
		"	(8) Memorized secret verifiers SHALL NOT permit the subscriber to store a "hint" that is accessible to an unauthenticated claimant.	Existing	P1	Agency	Both	Both
		"	(9) Verifiers SHALL NOT prompt subscribers to use specific types of information (e.g., "What was the name of your first pet?") when choosing memorized secrets.	Existing	P1	Agency	Both	Both
		"	(10) 10.When processing requests to establish and change memorized secrets, verifiers SHALL compare the prospective secrets against the list maintained as required by IA-5(1)(a)(1) that contains values known to be commonly used, expected, or compromised.	Existing	P1	Agency	Both	Both
		"	(11) If a chosen secret is found in the list, the CSP or verifier SHALL advise the subscriber that they need to select a different secret.	Existing	P1	Agency	Both	Both
		"	(12) If a chosen secret is found in the list, the CSP or verifier SHALL provide the reason for rejection.	Existing	P1	Agency	Both	Both
		"	(13) If a chosen secret is found in the list, the CSP or verifier SHALL require the subscriber to choose a different value.	Existing	P1	Agency	Both	Both
		"	(14) Verifiers SHALL implement a rate-limiting mechanism that effectively limits failed authentication attempts that can be made on the subscriber's account to no more than five.	Existing	P1	Agency	Both	Both

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
5.6: IA-5 (1)	IA-5 (1)	Authenticator Management Authenticator Types (continued)	(15) Verifiers SHALL force a change of memorized secret if there is evidence of compromise of the authenticator.	Existing	P1	Agency	Both	Both
		"	(16) The verifier SHALL use approved encryption when requesting memorized secrets in order to provide resistance to eavesdropping and MitM attacks.	Existing	P1	Agency	Both	Both
		"	(17) The verifier SHALL use an authenticated protected channel when requesting memorized secrets in order to provide resistance to eavesdropping and MitM attacks.	Existing	P1	Agency	Both	Both
		"	(18) Verifiers SHALL store memorized secrets in a form that is resistant to offline attacks.	Existing	P1	Agency	Both	Both
		"	(19) Memorized secrets SHALL be salted and hashed using a suitable one-way key derivation function.	Existing	P1	Agency	Both	Both
		"	(20) The salt SHALL be at least 32 bits in length and be chosen arbitrarily to minimize salt value collisions among stored hashes.	Existing	P1	Agency	Both	Both
		"	(21) Both the salt value and the resulting hash SHALL be stored for each subscriber using a memorized secret authenticator	Existing	P1	Agency	Both	Both
		"	(22) If an additional iteration of a key derivation function using a salt value known only to the verifier is performed, then this secret salt value SHALL be generated with an approved random bit generator and of sufficient length.	10/1/2024	P1	Agency	Both	Both
		"	(23) If an additional iteration of a key derivation function using a salt value known only to the verifier is performed, then this secret salt value SHALL provide at least the minimum-security strength.	10/1/2024	P1	Agency	Both	Both
		"	(24) If an additional iteration of a key derivation function using a salt value known only to the verifier is performed, then this secret salt value SHALL be stored separately from the memorized secrets.	10/1/2024	P1	Agency	Both	Both
		"	(b) Look-Up Secret Authenticators and Verifiers	10/1/2024	P1			
		"	(1) CSPs creating look-up secret authenticators SHALL use an approved random bit generator to generate the list of secrets.	10/1/2024	P1	Agency	Both	Both
		"	(2) Look-up secrets SHALL have at least 20 bits of entropy.	10/1/2024	P1	Agency	Both	Both
		"	(3) If look-up secrets are distributed online, then they SHALL be distributed over a secure channel in accordance with the post-enrollment binding requirements in IA-5 n 17 through 25.	10/1/2024	P1	Agency	Both	Both
		"	(4) Verifiers of look-up secrets SHALL prompt the claimant for the next secret from their authenticator or for a specific (e.g., numbered) secret.	10/1/2024	P1	Agency	Both	Both
		"	(5) A given secret from an authenticator SHALL be used successfully only once.	10/1/2024	P1	Agency	Both	Both
		"	(6) If a look-up secret is derived from a grid (bingo) card, then each cell of the grid SHALL be used only once.	10/1/2024	P1	Agency	Both	Both
		"	(7) Verifiers SHALL store look-up secrets in a form that is resistant to offline attacks.	10/1/2024	P1	Agency	Both	Both
		"	(8) If look-up secrets have at least 112 bits of entropy, then they SHALL be hashed with an approved one-way function	10/1/2024	P1	Agency	Both	Both
		"	(9) If look-up secrets have less than 112 bits of entropy, then they SHALL be salted and hashed using a suitable one-way key derivation function.	10/1/2024	P1	Agency	Both	Both
		"	(10) If look-up secrets have less than 112 bits of entropy, then the salt SHALL be at least 32 bits in length and be chosen arbitrarily to minimize salt value collisions among stored hashes.	10/1/2024	P1	Agency	Both	Both
		"	(11) If look-up secrets have less than 112 bits of entropy, then both the salt value and the resulting hash SHALL be stored for each look-up secret	10/1/2024	P1	Agency	Both	Both

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
5.6: IA-5 (1)	IA-5 (1)	Authenticator Management Authenticator Types (continued)	(12) If look-up secrets that have less than 64 bits of entropy, then the verifier SHALL implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber's account.	10/1/2024	P1	Agency	Both	Both
		"	(13) The verifier SHALL use approved encryption when requesting look-up secrets in order to provide resistance to eavesdropping and MitM attacks.	10/1/2024	P1	Agency	Both	Both
		"	(14) The verifier SHALL use an authenticated protected channel when requesting look-up secrets in order to provide resistance to eavesdropping and MitM attacks.	10/1/2024	P1	Agency	Both	Both
		"	(c) Out-of-Band Authenticators and Verifiers	10/1/2024	P1			
		"	(1) The out-of-band authenticator SHALL establish a separate channel with the verifier in order to retrieve the out-of-band secret or authentication request.	10/1/2024	P1	Agency	Both	Both
		"	(2) Communication over the secondary channel SHALL be encrypted unless sent via the public switched telephone network (PSTN).	10/1/2024	P1	Agency	Both	Both
		"	(3) Methods that do not prove possession of a specific device, such as voice-over-IP (VOIP) or email, SHALL NOT be used for out-of-band authentication.	10/1/2024	P1	Agency	Both	Both
		"	(4) If PSTN is not being used for out-of-band communication, then the out-of-band authenticator SHALL uniquely authenticate itself by establishing an authenticated protected channel with the verifier.	10/1/2024	P1	Agency	Both	Both
		"	(5) If PSTN is not being used for out-of-band communication, then the out-of-band authenticator SHALL communicate with the verifier using approved cryptography.	10/1/2024	P1	Agency	Both	Both
		"	(6) If PSTN is not being used for out-of-band communication, then the key used to authenticate the out-of-band device SHALL be stored in suitably secure storage available to the authenticator application (e.g., keychain storage, TPM, TEE, secure element).	10/1/2024	P1	Agency	Both	Both
		"	(7) If the PSTN is used for out-of-band authentication and a secret is sent to the out-of-band device via the PSTN, then the out-of-band authenticator SHALL uniquely authenticate itself to a mobile telephone network using a SIM card or equivalent that uniquely identifies the device.	10/1/2024	P1	Agency	Both	Both
		"	(8) If the out-of-band authenticator sends an approval message over the secondary communication channel, it SHALL either accept transfer of a secret from the primary channel to be sent to the verifier via the secondary communications channel, or present a secret received via the secondary channel from the verifier and prompt the claimant to verify the consistency of that secret with the primary channel, prior to accepting a yes/no response from the claimant which it sends to the verifier.	10/1/2024	P1	Agency	Both	Both
		"	(9) The verifier SHALL NOT store the identifying key itself, but SHALL use a verification method (e.g., an approved hash function or proof of possession of the identifying key) to uniquely identify the authenticator.	10/1/2024	P1	Agency	Both	Both
		"	(10) Depending on the type of out-of-band authenticator, one of the following SHALL take place: transfer of a secret to the primary channel, transfer of a secret to the secondary channel, or verification of secrets by the claimant.	10/1/2024	P1	Agency	Both	Both
		"	(11) If the out-of-band authenticator operates by transferring the secret to the primary channel, then the verifier SHALL transmit a random secret to the out-of-band authenticator and then wait for the secret to be returned on the primary communication channel.	10/1/2024	P1	Agency	Both	Both

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
5.6: IA-5 (1)	IA-5 (1)	Authenticator Management Authenticator Types (continued)	(12) If the out-of-band authenticator operates by transferring the secret to the secondary channel, then the verifier SHALL display a random authentication secret to the claimant via the primary channel and then wait for the secret to be returned on the secondary channel from the claimant's out-of- band authenticator.	10/1/2024	P1	Agency	Both	Both
		"	(13) If the out-of-band authenticator operates by verification of secrets by the claimant, then the verifier SHALL display a random authentication secret to the claimant via the primary channel, send the same secret to the out-of-band authenticator via the secondary channel for presentation to the claimant, and then wait for an approval (or disapproval) message via the secondary channel.	10/1/2024	P1	Agency	Both	Both
		"	(14) The authentication SHALL be considered invalid if not completed within 10 minutes.	10/1/2024	P1	Agency	Both	Both
		"	(15) Verifiers SHALL accept a given authentication secret only once during the validity period.	10/1/2024	P1	Agency	Both	Both
		"	(16) The verifier SHALL generate random authentication secrets with at least 20 bits of entropy.	10/1/2024	P1	Agency	Both	Both
		"	(17) The verifier SHALL generate random authentication secrets using an approved random bit generator.	10/1/2024	P1	Agency	Both	Both
		"	(18) If the authentication secret has less than 64 bits of entropy, the verifier SHALL implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber's account as described in IA-5 I (3) through (4).	10/1/2024	P1	Agency	Both	Both
		"	(19) If out-of-band verification is to be made using the PSTN, then the verifier SHALL verify that the pre-registered telephone number being used is associated with a specific physical device.	10/1/2024	P1	Agency	Both	Both
		"	(20) If out-of-band verification is to be made using the PSTN, then changing the pre-registered telephone number is considered to be the binding of a new authenticator and SHALL only occur as described in IA-5 n (17) through (25).	10/1/2024	P1	Agency	Both	Both
		"	(21) If PSTN is used for out-of-band authentication, then the CSP SHALL offer subscribers at least one alternate authenticator that is not RESTRICTED and can be used to authenticate at the required AAL.	10/1/2024	P1	Agency	Both	Both
		"	(22) If PSTN is used for out-of-band authentication, then the CSP SHALL Provide meaningful notice to subscribers regarding the security risks of the RESTRICTED authenticator and availability of alternative(s) that are not RESTRICTED.	10/1/2024	P1	Agency	Both	Both
		"	(23) If PSTN is used for out-of-band authentication, then the CSP SHALL address any additional risk to subscribers in its risk assessment.	10/1/2024	P1	Agency	Both	Both
		"	(24) If PSTN is used for out-of-band authentication, then the CSP SHALL develop a migration plan for the possibility that the RESTRICTED authenticator is no longer acceptable at some point in the future and include this migration plan in its digital identity acceptance statement.	10/1/2024	P1	Agency	Both	Both
		"	(d) OTP Authenticators and Verifiers	10/1/2024	P1			
		"	(1) The secret key and its algorithm SHALL provide at least the minimum security strength of 112 bits as of the date of this publication.	10/1/2024	P1	Agency	Both	Both
		"	(2) The nonce SHALL be of sufficient length to ensure that it is unique for each operation of the device over its lifetime.	10/1/2024	P1	Agency	Both	Both
		"	(3) OTP authenticators — particularly software-based OTP generators —SHALL NOT facilitate the cloning of the secret key onto multiple devices.	10/1/2024	P1	Agency	Both	Both

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
5.6: IA-5 (1)	IA-5 (1)	Authenticator Management Authenticator Types (continued)	(4) The authenticator output SHALL have at least 6 decimal digits (approximately 20 bits) of entropy.	Existing	P1	Agency	Both	Both
		"	(5) If the nonce used to generate the authenticator output is based on a real-time clock, then the nonce SHALL be changed at least once every 2 minutes.	10/1/2024	P1	Agency	Both	Both
		"	(6) The OTP value associated with a given nonce SHALL be accepted only once.	Existing	P1	Agency	Both	Both
		"	(7) The symmetric keys used by authenticators are also present in the verifier and SHALL be strongly protected against compromise.	10/1/2024	P1	Agency	Both	Both
		"	(8) If a single-factor OTP authenticator is being associated with a subscriber account, then the verifier or associated CSP SHALL use approved cryptography to either generate and exchange or to obtain the secrets required to duplicate the authenticator output.	10/1/2024	P1	Agency	Both	Both
		"	(9) The verifier SHALL use approved encryption when collecting the OTP.	10/1/2024	P1	Agency	Both	Both
		"	(10) The verifier SHALL use an authenticated protected channel when collecting the OTP.	10/1/2024	P1	Agency	Both	Both
		"	(11) If a time-based OTP is used, it SHALL have a defined lifetime (recommended 30 seconds) that is determined by the expected clock drift — in either direction — of the authenticator over its lifetime, plus allowance for network delay and user entry of the OTP.	10/1/2024	P1	Agency	Both	Both
		"	(12) Verifiers SHALL accept a given time-based OTP only once during the validity period.	10/1/2024	P1	Agency	Both	Both
		"	(13) If the authenticator output has less than 64 bits of entropy, the verifier SHALL implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber's account as described in IA-5 I (3) through (4).	10/1/2024	P1	Agency	Both	Both
		"	(14) If the authenticator is multi-factor, then each use of the authenticator SHALL require the input of the additional factor.	10/1/2024	P1	Agency	Both	Both
		"	(15) If the authenticator is multi-factor and a memorized secret is used by the authenticator for activation, then that memorized secret SHALL be a randomly chosen numeric secret at least 6 decimal digits in length or other memorized secret meeting the requirements of IA-5 (1)(a).	10/1/2024	P1	Agency	Both	Both
		"	(16) If the authenticator is multi-factor, then use of a memorized secret for activation SHALL be rate limited as specified in IA-5 I (3) through (4).	10/1/2024	P1	Agency	Both	Both
		"	(17) If the authenticator is multi-factor and is activated by a biometric factor, then that factor SHALL meet the requirements of IA-5 m, including limits on the number of consecutive authentication failures.	10/1/2024	P1	Agency	Both	Both
		"	(18) If the authenticator is multi-factor, then the unencrypted key and activation secret or biometric sample — and any biometric data derived from the biometric sample such as a probe produced through signal processing — SHALL be zeroized immediately after an OTP has been generated.	10/1/2024	P1	Agency	Both	Both
		"	(19) If the authenticator is multi-factor, the verifier or CSP SHALL establish, via the authenticator source, that the authenticator is a multi-factor device.	10/1/2024	P1	Agency	Both	Both
		"	(20) In the absence of a trusted statement that it is a multi-factor device, the verifier SHALL treat the authenticator as single-factor, in accordance with IA-5 (1) (d) (1) through (13).	10/1/2024	P1	Agency	Both	Both
		"	(e) Cryptographic Authenticators and Verifiers (including single- and multi-factor cryptographic authenticators, both hardware- and software-based)	10/1/2024	P1			

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
5.6: IA-5 (1)	IA-5 (1)	Authenticator Management Authenticator Types (continued)	(1) If the cryptographic authenticator is software based, the key SHALL be stored in suitably secure storage available to the authenticator application.	10/1/2024	P1	Agency	Both	Both
		"	(2) If the cryptographic authenticator is software based, the key SHALL be strongly protected against unauthorized disclosure by the use of access controls that limit access to the key to only those software components on the device requiring access.	10/1/2024	P1	Agency	Both	Both
		"	(3) If the cryptographic authenticator is software based, it SHALL NOT facilitate the cloning of the secret key onto multiple devices.	10/1/2024	P1	Agency	Both	Both
		"	(4) If the authenticator is single-factor and hardware-based, secret keys unique to the device SHALL NOT be exportable (i.e., cannot be removed from the device).	10/1/2024	P1	Agency	Both	Both
		"	(5) If the authenticator is hardware-based, the secret key and its algorithm SHALL provide at least the minimum-security length of 112 bits as of the date of this publication.	10/1/2024	P1	Agency	Both	Both
		"	(6) If the authenticator is hardware-based, the challenge nonce SHALL be at least 64 bits in length.	10/1/2024	P1	Agency	Both	Both
		"	(7) If the authenticator is hardware-based, approved cryptography SHALL be used.	10/1/2024	P1	Agency	Both	Both
		"	(8) Cryptographic keys stored by the verifier SHALL be protected against modification.	10/1/2024	P1	Agency	Both	Both
		"	(9) If symmetric keys are used, cryptographic keys stored by the verifier SHALL be protected against disclosure.	10/1/2024	P1	Agency	Both	Both
		"	(10) The challenge nonce SHALL be at least 64 bits in length.	10/1/2024	P1	Agency	Both	Both
		"	(11) The challenge nonce SHALL either be unique over the authenticator's lifetime or statistically unique (i.e., generated using an approved random bit generator).	10/1/2024	P1	Agency	Both	Both
		"	(12) The verification operation SHALL use approved cryptography.	10/1/2024	P1	Agency	Both	Both
		"	(13) If a multi-factor cryptographic software authenticator is being used, then each authentication requires the presentation of the activation factor.	10/1/2024	P1	Agency	Both	Both
		"	(14) If the authenticator is multi-factor, then any memorized secret used by the authenticator for activation SHALL be a randomly chosen numeric secret at least 6 decimal digits in length or other memorized secret meeting the requirements of IA-5 (1) (a).	10/1/2024	P1	Agency	Both	Both
		"	(15) If the authenticator is multi-factor, then use of a memorized secret for activation SHALL be rate limited as specified in IA-5 I (3) through (4).	10/1/2024	P1	Agency	Both	Both
		"	(16) If the authenticator is multi-factor and is activated by a biometric factor, then that factor SHALL meet the requirements of IA-5 m, including limits on the number of consecutive authentication failures.	10/1/2024	P1	Agency	Both	Both
		"	(17) If the authenticator is multi-factor, then the unencrypted key and activation secret or biometric sample — and any biometric data derived from the biometric sample such as a probe produced through signal processing — SHALL be zeroized immediately after an authentication transaction has taken place.	10/1/2024	P1	Agency	Both	Both
5.6: IA-5 (2)	IA-5 (2)	Authenticator Management Public Key Based Authentication	(a) For public key-based authentication:	Existing	P1			
		"	(1) Enforce authorized access to the corresponding private key; and	Existing	P1	Agency	Both	Both
		"	(2) Map the authenticated identity to the account of the individual or group; and	Existing	P1	Agency	Both	Both
		"	(b) When public key infrastructure (PKI) is used:	Existing	P1	Agency	Both	Both

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
5.6: IA-5 (2)	IA-5 (2)	Authenticator Management Public Key Based Authentication (continued)	(1) Validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; and	Existing	P1	Agency	Both	Both
		"	(2) Implement a local cache of revocation data to support path discovery and validation.	Existing	P1	Agency	Both	Both
5.6: IA-5 (6)	IA-5 (6)	Authenticator Management Protection of Authenticators	Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access.	Existing	P1	Agency	Both	Both
5.6: IA-6	IA-6	Authentication Feedback	Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.	Existing	P3	Agency	Both	Both
5.6: IA-7	IA-7	Cryptographic Module Authentication	Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.	Zero-cycle	P2	Agency	Both	Both
5.6: IA-8	IA-8	Identification and Authentication (Non-Organizational Users)	Control: Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.	Zero-cycle	P2	Agency	Both	Both
5.6: IA-8 (1)	IA-8 (1)	Identification and Authentication (Non-Organizational Users) Acceptance of PIV Credentials From Other Agencies	Accept and electronically verify Personal Identity Verification-compliant credentials from other federal, state, local, tribal, or territorial (SLTT) agencies.	Zero-cycle	P2	Agency	Both	Both
5.6: IA-8 (2)	IA-8 (2)	Identification and Authentication (Non-Organizational Users) Acceptance of External Authenticators	(a) Accept only external authenticators that are NIST-compliant; and	Zero-cycle	P2	Agency	Both	Both
		"	(b) Document and maintain a list of accepted external authenticators.	Zero-cycle	P2	Agency	Both	Both
5.6: IA-8 (4)	IA-8 (4)	Identification and Authentication (Non-Organizational Users) Use of Defined Profiles	Conform to the following profiles for identity management: Security Assertion Markup Language (SAML) or OpenID Connect.	Zero-cycle	P2	Agency	Both	Both
5.6: IA-11	IA-11	Re-Authentication	Require users to re-authenticate when: roles, authenticators, or credentials change, security categories of systems change, the execution of privileged functions occur, or every 12 hours.	Zero-cycle	P2	Agency	Both	Both
5.6: IA-12	IA-12	Identity Proofing	a. Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines;	Zero-cycle	P2	Agency	Both	Both
		"	b. Resolve user identities to a unique individual; and	Zero-cycle	P2	Agency	Both	Both
		"	c. Collect, validate, and verify identity evidence.	Zero-cycle	P2	Agency	Both	Both
5.6: IA-12 (2)	IA-12 (2)	Identity Proofing Identity Evidence	Require evidence of individual identification be presented to the registration authority.	Zero-cycle	P2	Agency	Both	Both
5.6: IA-12 (3)	IA-12 (3)	Identity Proofing Identity Evidence Validation and Verification	a. Require that the presented identity evidence be validated and verified through agency defined resolution, validation, and verification methods.	Zero-cycle	P2	Agency	Both	Both
		"	b. Identity proofing SHALL NOT be performed to determine suitability or entitlement to gain access to services or benefits.	Zero-cycle	P2	Agency	Both	Both
		"	c. 1. Collection of PII SHALL be limited to the minimum necessary to resolve to a unique identity in a given context.	Zero-cycle	P2	Agency	Both	Both
		"	2. Collection of PII SHALL be limited to the minimum necessary to validate the existence of the claimed identity and associate the claimed identity with the applicant providing identity evidence for appropriate identity resolution, validation, and verification.	Zero-cycle	P2	Agency	Both	Both

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
5.6: IA-12 (3)	IA-12 (3)	Identity Proofing Identity Evidence Validation and Verification (continued)	d. The CSP SHALL provide explicit notice to the applicant at the time of collection regarding the purpose for collecting and maintaining a record of the attributes necessary for identity proofing, including whether such attributes are voluntary or mandatory to complete the identity proofing process, and the consequences for not providing the attributes.	Zero-cycle	P2	Agency	Both	Both
		"	e. If CSPs process attributes for purposes other than identity proofing, authentication, or attribute assertions (collectively "identity service"), related fraud mitigation, or to comply with law or legal process, then CSPs SHALL implement measures to maintain predictability and manageability commensurate with the privacy risk arising from the additional processing.	Zero-cycle	P2	Agency	Both	Both
		"	f. If the CSP employs consent as part of its measures to maintain predictability and manageability, ...then it SHALL NOT make consent for the additional processing a condition of the identity service.	Zero-cycle	P2	Agency	Both	Both
		"	g. The CSP SHALL provide mechanisms for redress of applicant complaints or problems arising from the identity proofing.	Zero-cycle	P2	Agency	Both	Both
		"	These [redress] mechanisms SHALL be easy for applicants to find and use.	Zero-cycle	P2	Agency	Both	Both
		"	h. The CSP SHALL assess the [redress] mechanisms for their efficacy in achieving resolution of complaints or problems.	Zero-cycle	P2	Agency	Both	Both
		"	i. The identity proofing and enrollment processes SHALL be performed according to an applicable written policy or "practice statement" that specifies the particular steps taken to verify identities.	Zero-cycle	P2	Agency	Both	Both
		"	j. The "practice statement" SHALL include control information detailing how the CSP handles proofing errors that result in an applicant not being successfully enrolled.	Zero-cycle	P2	Agency	Both	Both
		"	k. The CSP SHALL maintain a record, including audit logs, of all steps taken to verify the identity of the applicant as long as the identity exists in the information system.	Zero-cycle	P2	Agency	Both	Both
		"	l. The CSP SHALL record the types of identity evidence presented in the proofing process.	Zero-cycle	P2	Agency	Both	Both
		"	m. The CSP SHALL conduct a risk management process, including assessments of privacy and security risks to determine:	Zero-cycle	P2	Agency	Both	Both
		"	1. Any steps that it will take to verify the identity of the applicant beyond any mandatory requirements specified herein;	Zero-cycle	P2	Agency	Both	Both
		"	2. The PII, including any biometrics, images, scans, or other copies of the identity evidence that the CSP will maintain as a record of identity proofing (Note: Specific federal requirements may apply); and	Zero-cycle	P2	Agency	Both	Both
		"	3. The schedule of retention for these records (Note: CSPs may be subject to specific retention policies in accordance with applicable laws, regulations, or policies, including any National Archives and Records Administration (NARA) records retention schedules that may apply).	Zero-cycle	P2	Agency	Both	Both
		"	n. All PII collected as part of the enrollment process SHALL be protected to ensure confidentiality, integrity, and attribution of the information source.	Zero-cycle	P2	Agency	Both	Both
		"	o. "The entire proofing transaction, including transactions that involve a third party, SHALL occur over authenticated protected channels. "	Zero-cycle	P2	Agency	Both	Both
		"	p. "If the CSP uses fraud mitigation measures, then the CSP SHALL conduct a privacy risk assessment for these mitigation measures. "	Zero-cycle	P2	Agency	Both	Both

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
5.6: IA-12 (3)	IA-12 (3)	Identity Proofing Identity Evidence Validation and Verification (continued)	Such assessments SHALL include any privacy risk mitigations (e.g., risk acceptance or transfer, limited retention, use limitations, notice) or other technological mitigations (e.g., cryptography), and be documented per requirement IA-12(3) k – m above.	Zero-cycle	P2	Agency	Both	Both
		"	q. In the event a CSP ceases to conduct identity proofing and enrollment processes, then the CSP SHALL be responsible for fully disposing of or destroying any sensitive data including PII, or its protection from unauthorized access for the duration of retention.	Zero-cycle	P2	Agency	Both	Both
		"	r. Regardless of whether the CSP is a federal agency or non- federal entity, the following requirements apply to the federal agency offering or using the proofing service:	Zero-cycle	P2	Agency	Both	Both
		"	1. The agency SHALL consult with their Senior Agency Official for Privacy (SAOP) to conduct an analysis determining whether the collection of PII to conduct identity proofing triggers Privacy Act requirements.	Zero-cycle	P2	Agency	Both	Both
		"	2. The agency SHALL publish a System of Records Notice (SORN) to cover such collection, as applicable.	Zero-cycle	P2	Agency	Both	Both
		"	3. The agency SHALL consult with their SAOP to conduct an analysis determining whether the collection of PII to conduct identity proofing triggers E-Government Act of 2002 requirements.	Zero-cycle	P2	Agency	Both	Both
		"	4. The agency SHALL publish a Privacy Impact Assessment (PIA) to cover such collection, as applicable.	Zero-cycle	P2	Agency	Both	Both
		"	s. An enrollment code SHALL be comprised of one of the following:	Zero-cycle	P2	Agency	Both	Both
		"	1. Minimally, a random six character alphanumeric or equivalent entropy. For example, a code generated using an approved random number generator or a serial number for a physical hardware authenticator; OR	Zero-cycle	P2	Agency	Both	Both
		"	2. A machine-readable optical label, such as a QR Code, that contains data of similar or higher entropy as a random six character alphanumeric.	Zero-cycle	P2	Agency	Both	Both
		"	t. Training requirements for personnel validating evidence SHALL be based on the policies, guidelines, or requirements of the CSP or RP.	Zero-cycle	P2	Agency	Both	Both
		"	u. This criterion applies to CSPs that provide identity proofing and enrollment services to minors (under the age of 18):	Zero-cycle	P2	Agency	Both	Both
		"	If the CSP provides identity proofing and enrollment services to minors (under the age of 18), then...the CSP SHALL give special consideration to the legal restrictions of interacting with minors unable to meet the evidence requirements of identity proofing [to ensure compliance with the Children's Online Privacy Protection Act of 1998 (COPPA), and other laws, as applicable]. "	Zero-cycle	P2	Agency	Both	Both
		"	Requirements v and w apply to the collection of biometric characteristics for in-person (physical or supervised remote) identity proofing and are mandatory at IAL3. These criteria also apply to CSPs that optionally choose to collect biometric characteristics through in-person identity-proofing identity proofing and enrollment at IAL2.					
		"	v. The CSP SHALL have the operator view the biometric source (e.g., fingers, face) for presence of non-natural materials and perform such inspections as part of the proofing process.	Zero-cycle	P2	Agency	Both	Both
		"	w. The CSP SHALL collect biometrics in such a way that ensures that the biometric is collected from the applicant, and not another subject. All biometric performance requirements in IA-5 m (1) through (12) apply.	Zero-cycle	P2	Agency	Both	Both
		"	x. The CSP SHALL support in-person or remote identity proofing, or both.	Zero-cycle	P2	Agency	Both	Both
		"	y. The CSP SHALL collect the following from the applicant:	Zero-cycle	P2	Agency	Both	Both

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
5.6: IA-12 (3)	IA-12 (3)	Identity Proofing Identity Evidence Validation and Verification (continued)	1. One piece of SUPERIOR or STRONG evidence if the evidence's issuing source, during its identity proofing event, confirmed the claimed identity by collecting two or more forms of SUPERIOR or STRONG evidence and the CSP validates the evidence directly with the issuing source; OR	Zero-cycle	P2	Agency	Both	Both
		"	2. Two pieces of STRONG evidence; OR	Zero-cycle	P2	Agency	Both	Both
		"	3. One piece of STRONG evidence plus two pieces of FAIR evidence	Zero-cycle	P2	Agency	Both	Both
		"	z. The CSP SHALL validate each piece of evidence with a process that can achieve the same strength as the evidence presented (see 'z' above). For example, if two forms of STRONG identity evidence are presented, each piece of evidence will be validated at a strength of STRONG.	Zero-cycle	P2	Agency	Both	Both
		"	aa. The CSP SHALL verify identity evidence as follows:	Zero-cycle	P2	Agency	Both	Both
		"	At a minimum, the applicant's binding to identity evidence must be verified by a process that is able to achieve a strength of STRONG.	Zero-cycle	P2	Agency	Both	Both
		"	bb. For IAL2 remote proofing: The collection of biometric characteristics for physical or biometric comparison of the applicant to the strongest piece of identity evidence provided to support the claimed identity performed remotely SHALL adhere to all requirements as specified in IA-5 m.	Zero-cycle	P2	Agency	Both	Both
		"	cc. Knowledge-based verification (KBV) SHALL NOT be used for in-person (physical or supervised remote) identity verification.	Zero-cycle	P2	Agency	Both	Both
		"	dd. The CSP SHALL employ appropriately tailored security controls, to include control enhancements, from the moderate or high baseline of security controls defined in the CJIS Security Policy.	Zero-cycle	P2	Agency	Both	Both
		"	The CSP SHALL ensure that the minimum assurance-related controls for moderate-impact systems are satisfied.	Zero-cycle	P2	Agency	Both	Both
		"	ee. Supervised Remote Identity Proofing: Supervised remote identity proofing is intended to provide controls for comparable levels of confidence and security to in-person IAL3 identity proofing for identity proofing processes that are performed remotely. Supervised remote identity proofing is optional for CSPs; that is, if a CSP chooses to use supervised remote identity proofing, then the following requirements, (1) through (8), would apply. It should be noted that the term "supervised remote identity proofing" has specialized meaning and is used only to refer to the specialized equipment and the following control requirements, (1) through (8). In addition to those requirements presented in this document, as well as the applicable identity validation and verification requirements, CSPs that provide supervised remote identity proofing services must demonstrate conformance with the requirements contained in this section. The following requirements for supervised remote proofing apply specifically to IAL3. If the equipment/facilities used for supervised remote proofing are used for IAL2 identity proofing, the following requirements, (1) through (8), for supervised remote proofing do not apply. In this case, the requirements for conventional remote identity proofing are applicable.	Zero-cycle	P2	Agency	Both	Both
		"	(1) Supervised remote identity proofing and enrollment transactions SHALL meet the following requirements, in addition to the IAL3 validation and verification requirements specified in IA-12(3)s.	Zero-cycle	P2	Agency	Both	Both
		"	(2) The CSP SHALL monitor the entire identity proofing session, from which the applicant SHALL NOT depart — for example, by a continuous high-resolution video transmission of the applicant.	Zero-cycle	P2	Agency	Both	Both
		"	(3) The CSP SHALL have a live operator participate remotely with the applicant for the entirety of the identity proofing session.	Zero-cycle	P2	Agency	Both	Both

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
5.6: IA-12 (3)	IA-12 (3)	Identity Proofing Identity Evidence Validation and Verification (continued)	(4) The CSP SHALL require all actions taken by the applicant during the identity proofing session to be clearly visible to the remote operator.	Zero-cycle	P2	Agency	Both	Both
		"	(5) The CSP SHALL require that all digital validation of evidence (e.g., via chip or wireless technologies) be performed by integrated scanners and sensors.	Zero-cycle	P2	Agency	Both	Both
		"	(6) The CSP SHALL require operators to have undergone a training program to detect potential fraud and to properly perform a supervised remote proofing session.	Zero-cycle	P2	Agency	Both	Both
		"	(7) The CSP SHALL employ physical tamper detection and resistance features appropriate for the environment in which it is located.	Zero-cycle	P2	Agency	Both	Both
		"	(8) The CSP SHALL ensure that all communications occur over a mutually authenticated protected channel.	Zero-cycle	P2	Agency	Both	Both
		"	ff. Trusted Referee: The use of trusted referees is optional for CSPs; that is, if a CSP chooses to use trusted referees for identity proofing and enrollment, then the following requirements, (1) through (3) would apply. The use of trusted referees is intended to assist in the identity proofing and enrollment for populations that are unable to meet IAL2 identity proofing requirements, or otherwise would be challenged to perform identity proofing and enrollment process requirements. Such populations may include, but are not limited to:	Zero-cycle	P2	Agency	Both	Both
		"	· disabled individuals;	Zero-cycle	P2	Agency	Both	Both
		"	· elderly individuals;	Zero-cycle	P2	Agency	Both	Both
		"	· homeless individuals,	Zero-cycle	P2	Agency	Both	Both
		"	· individuals with little or no access to online services or computing devices;	Zero-cycle	P2	Agency	Both	Both
		"	· unbanked and individuals with little or no credit history;	Zero-cycle	P2	Agency	Both	Both
		"	· victims of identity theft;	Zero-cycle	P2	Agency	Both	Both
		"	· children under 18; and	Zero-cycle	P2	Agency	Both	Both
		"	· immigrants.	Zero-cycle	P2	Agency	Both	Both
		"	In addition to those requirements presented in the General section of this document, as well as the applicable IAL requirements, CSPs that use trusted referees in their identity proofing services must demonstrate conformance with the requirements contained in this section.					
		"	(1) If the CSP uses trusted referees, then...The CSP SHALL establish written policy and procedures as to how a trusted referee is determined and the lifecycle by which the trusted referee retains their status as a valid referee, to include any restrictions, as well as any revocation and suspension requirements.	Zero-cycle	P2	Agency	Both	Both
		"	(2) If the CSP uses trusted referees, then...The CSP SHALL proof the trusted referee at the same IAL as the applicant proofing.	Zero-cycle	P2	Agency	Both	Both
		"	(3) If the CSP uses trusted referees, then...The CSP SHALL determine the minimum evidence required to bind the relationship between the trusted referee and the applicant.	Zero-cycle	P2	Agency	Both	Both

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
5.6: IA-12 (5)	IA-12 (5)	(5) Identity Proofing Address Confirmation	a. Require that a registration code <u>or</u> notice of proofing be delivered through an out-of-band channel to verify the users address (physical or digital) of record.	Zero-cycle	P2	Agency	Both	Both
		"	b. The CSP SHALL confirm address of record.	Zero-cycle	P2	Agency	Both	Both
		"	c. Valid records to confirm address SHALL be issuing source(s) or authoritative source(s).	Zero-cycle	P2	Agency	Both	Both
		"	Self-asserted address data that has not been confirmed in records SHALL NOT be used for confirmation.	Zero-cycle	P2	Agency	Both	Both
		"	d. Note that IAL2-7 applies only to in-person proofing at IAL2.	Zero-cycle	P2	Agency	Both	Both
		"	If the CSP performs in-person proofing for IAL2 and provides an enrollment code directly to the subscriber for binding to an authenticator at a later time, then the enrollment code...SHALL be valid for a maximum of seven (7) days.	Zero-cycle	P2	Agency	Both	Both
		"	e. For remote identity proofing at IAL2:	Zero-cycle	P2	Agency	Both	Both
		"	The CSP SHALL send an enrollment code to a confirmed address of record for the applicant.	Zero-cycle	P2	Agency	Both	Both
		"	f. For remote identity proofing at IAL2:	Zero-cycle	P2	Agency	Both	Both
		"	The applicant SHALL present a valid enrollment code to complete the identity proofing process.	Zero-cycle	P2	Agency	Both	Both
		"	g. Note that the following enrollment code validity periods apply to enrollment codes sent to confirmed addresses of record for IAL2 remote in-person proofing only.	Zero-cycle	P2	Agency	Both	Both
		"	Enrollment codes shall have the following maximum validities:	Zero-cycle	P2	Agency	Both	Both
		"	i. 10 days, when sent to a postal address of record within the contiguous United States;	Zero-cycle	P2	Agency	Both	Both
		"	ii. 30 days, when sent to a postal address of record outside the contiguous United States;	Zero-cycle	P2	Agency	Both	Both
		"	iii. 10 minutes, when sent to a telephone of record (SMS or voice);	Zero-cycle	P2	Agency	Both	Both
		"	iv. 24 hours, when sent to an email address of record.	Zero-cycle	P2	Agency	Both	Both
		"	h. If the enrollment code sent to the confirmed address of record as part of the remote identity proofing process at IAL2 is also intended to be an authentication factor, then...it SHALL be reset upon first use.	Zero-cycle	P2	Agency	Both	Both
		"	i. If the CSP performs remote proofing at IAL2 and optionally sends notification of proofing in addition to sending the required enrollment code, then...The CSP SHALL ensure the enrollment code and notification of proofing are sent to different addresses of record.	Zero-cycle	P2	Agency	Both	Both

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy: Incident Response (IR)								
IR-1	IR-1	POLICY AND PROCEDURES	a. Develop, document, and disseminate to all personnel when their unescorted logical or physical access to any information system results in the ability, right, or privilege to view, modify, or make use of unencrypted CJI:	Existing	P2	Both	Both	Both
		"	1. Agency-level incident response policy that:	Existing	P2	Both	Both	Both
		"	(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Existing	P2	Both	Both	Both
		"	(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and	Existing	P2	Both	Both	Both
		"	2. Procedures to facilitate the implementation of the incident response policy and the associated incident response controls;	Existing	P2	Both	Both	Both
		"	b. Designate an individual with security responsibilities to manage the development, documentation, and dissemination of the incident response policy and procedures; and	Existing	P2	Both	Both	Both
		"	c. Review and update the current incident response:	Zero-cycle	P2	Both	Both	Both
		"	1. Policy annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI; and	Zero-cycle	P2	Both	Both	Both
		"	2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.	Zero-cycle	P2	Both	Both	Both
IR-2	IR-2	INCIDENT RESPONSE TRAINING	a. Provide incident response training to system users consistent with assigned roles and responsibilities:	Existing	P2	Both	Both	Both
		"	1. Prior to assuming an incident response role or responsibility or acquiring system access;	Existing	P2	Both	Both	Both
		"	2. When required by system changes; and	Existing	P2	Both	Both	Both
		"	3. Annually thereafter; and	Existing	P2	Both	Both	Both
		"	b. Review and update incident response training content annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.	Zero-cycle	P3	Both	Both	Both
IR-2 (3)	IR-2 (3)	(3) INCIDENT RESPONSE TRAINING BREACH	Provide incident response training on how to identify and respond to a breach, including the organization’s process for reporting a breach.	Zero-cycle	P3	Both	Both	Both
IR-3	IR-3	INCIDENT RESPONSE TESTING	Test the effectiveness of the incident response capability for the system annually using the following tests: tabletop or walk-through exercises; simulations; or other agency-appropriate tests.	Zero-cycle	P3	Both	Both	Both
IR-3 (2)	IR-3 (2)	(2) INCIDENT RESPONSE TESTING COORDINATION WITH RELATED PLANS	Coordinate incident response testing with organizational elements responsible for related plans.	Zero-cycle	P3	Both	Both	Both
IR-4	IR-4	INCIDENT HANDLING	a. Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery;	Existing	P2	Both	Both	Both
		"	b. Coordinate incident handling activities with contingency planning activities;	Existing	P2	Both	Both	Both
		"	c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly; and	Existing	P2	Both	Both	Both
		"	d. Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.	Existing	P2	Both	Both	Both
IR-4 (1)	IR-4 (1)	(1) INCIDENT HANDLING AUTOMATED INCIDENT HANDLING PROCESSES	Support the incident handling process using automated mechanisms (e.g., online incident management systems and tools that support the collection of live response data, full network packet capture, and forensic analysis.	Existing	P2	Both	Both	Both
IR-5	IR-5	INCIDENT MONITORING	Track and document incidents.	Existing	P2	Both	Both	Both

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
IR-6	IR-6	INCIDENT REPORTING	a. Require personnel to report suspected incidents to the organizational incident response capability immediately but not to exceed one (1) hour after discovery; and	Zero-cycle	P2	Both	Both	Both
		"	b. Report incident information to organizational personnel with incident handling responsibilities, and if confirmed, notify the CSO, SIB Chief, or Interface Agency Official.	Zero-cycle	P2	Both	Both	Both
IR-6 (1)	IR-6 (1)	(1) INCIDENT REPORTING AUTOMATED REPORTING	Report incidents using automated mechanisms.	Existing	P2	Both	Both	Both
IR-6 (3)	IR-6 (3)	(3) INCIDENT REPORTING SUPPLY CHAIN COORDINATION	Provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident.	Zero-cycle	P2	Both	Both	Both
IR-7	IR-7	INCIDENT RESPONSE ASSISTANCE	Provide an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the system for the handling and reporting of incidents.	Existing	P3	Both	Both	Both
IR-7 (1)	IR-7 (1)	(1) INCIDENT RESPONSE ASSISTANCE AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION AND SUPPORT	Increase the availability of incident response information and support using automated mechanisms described in the discussion.	Zero-cycle	P3	Both	Both	Both
IR-8	IR-8	INCIDENT RESPONSE PLAN	a. Develop an incident response plan that:	Existing	P2	Both	Both	Both
		"	1. Provides the organization with a roadmap for implementing its incident response capability;	Existing	P2	Both	Both	Both
		"	2. Describes the structure and organization of the incident response capability;	Existing	P2	Both	Both	Both
		"	3. Provides a high-level approach for how the incident response capability fits into the overall organization;	Existing	P2	Both	Both	Both
		"	4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;	Existing	P2	Both	Both	Both
		"	5. Defines reportable incidents;	Existing	P2	Both	Both	Both
		"	6. Provides metrics for measuring the incident response capability within the organization;	Existing	P2	Both	Both	Both
		"	7. Defines the resources and management support needed to effectively maintain and mature an incident response capability;	Existing	P2	Both	Both	Both
		"	8. Addresses the sharing of incident information;	Existing	P2	Both	Both	Both
		"	9. Is reviewed and approved by the organization's/agency's executive leadership annually; and	Existing	P2	Both	Both	Both
		"	10. Explicitly designates responsibility for incident response to organizational personnel with incident reporting responsibilities and CSO or CJIS WAN Official.	Existing	P2	Both	Both	Both
		"	b. Distribute copies of the incident response plan to organizational personnel with incident handling responsibilities;	Existing	P2	Both	Both	Both
		"	c. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing;	Existing	P2	Both	Both	Both
		"	d. Communicate incident response plan changes to organizational personnel with incident handling responsibilities; and	Existing	P2	Both	Both	Both
		"	e. Protect the incident response plan from unauthorized disclosure and modification.	Existing	P2	Both	Both	Both
IR-8 (1)	IR-8 (1)	(1) INCIDENT RESPONSE PLAN BREACHES	Include the following in the Incident Response Plan for breaches involving personally identifiable information:	Zero-cycle	P2	Both	Both	Both
		"	(a) A process to determine if notice to individuals or other organizations, including oversight organizations, is needed;	Zero-cycle	P2	Both	Both	Both
		"	(b) An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms; and	Zero-cycle	P2	Both	Both	Both
		"	(c) Identification of applicable privacy requirements.	Zero-cycle	P2	Both	Both	Both

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy: Maintenance (MA)								
MA-1	MA-1	POLICY AND PROCEDURES	a. Develop, document, and disseminate to organizational personnel with system maintenance responsibilities:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. Agency-level maintenance policy that:	Zero-cycle	P2	TBD	TBD	TBD
		"	(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Zero-cycle	P2	TBD	TBD	TBD
		"	(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and	Zero-cycle	P2	TBD	TBD	TBD
		"	2. Procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls;	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Designate organizational personnel with information security and privacy responsibilities to manage the development, documentation, and dissemination of the maintenance policy and procedures; and	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Review and update the current maintenance:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. Policy annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI; and	Zero-cycle	P2	TBD	TBD	TBD
		"	2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.	Zero-cycle	P2	TBD	TBD	TBD
MA-2	MA-2	CONTROLLED MAINTENANCE	a. Schedule, document, and review records of maintenance, repair, and replacement on system components in accordance with manufacturer or vendor specifications and/or organizational requirements;	Zero-cycle	P3	TBD	TBD	TBD
		"	b. Approve and monitor all maintenance activities, whether performed on site or remotely and whether the system or system components are serviced on site or removed to another location;	Zero-cycle	P3	TBD	TBD	TBD
		"	c. Require that organizational personnel with information security and privacy responsibilities explicitly approve the removal of the system or system components from organizational facilities for off-site maintenance, repair, or replacement;	Zero-cycle	P3	TBD	TBD	TBD
		"	d. Sanitize equipment to remove information from associated media prior to removal from organizational facilities for off-site maintenance, repair, replacement, or destruction;	Zero-cycle	P3	TBD	TBD	TBD
		"	e. Check all potentially impacted controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions; and	Zero-cycle	P3	TBD	TBD	TBD
		"	f. Include the following information in organizational maintenance records:	Zero-cycle	P3	TBD	TBD	TBD
		"	1. Component name	Zero-cycle	P3	TBD	TBD	TBD
		"	2. Component serial number	Zero-cycle	P3	TBD	TBD	TBD
		"	3. Date/time of maintenance	Zero-cycle	P3	TBD	TBD	TBD
		"	4. Maintenance performed	Zero-cycle	P3	TBD	TBD	TBD
		"	5. Name(s) of entity performing maintenance including escort if required.	Zero-cycle	P3	TBD	TBD	TBD
MA-3	MA-3	MAINTENANCE TOOLS	a. Approve, control, and monitor the use of system maintenance tools; and	Zero-cycle	P4	TBD	TBD	TBD
		"	b. Review previously approved system maintenance tools prior to each use.	Zero-cycle	P4	TBD	TBD	TBD
MA-3(1)	MA-3(1)	(1) MAINTENANCE TOOLS INSPECT TOOLS	Inspect the maintenance tools used by maintenance personnel for improper or unauthorized modifications.	Zero-cycle	P4	TBD	TBD	TBD
MA-3(2)	MA-3(2)	(2) MAINTENANCE TOOLS INSPECT MEDIA	Check media containing diagnostic and test programs for malicious code before the media are used in the system.	Zero-cycle	P4	TBD	TBD	TBD

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
MA-3(3)	MA-3(3)	(3) MAINTENANCE TOOLS PREVENT UNAUTHORIZED REMOVAL	Prevent the removal of maintenance equipment containing organizational information by:	Zero-cycle	P4	TBD	TBD	TBD
		"	(a) Verifying that there is no organizational information contained on the equipment;	Zero-cycle	P4	TBD	TBD	TBD
		"	(b) Sanitizing or destroying the equipment;	Zero-cycle	P4	TBD	TBD	TBD
		"	(c) Retaining the equipment within the facility; or	Zero-cycle	P4	TBD	TBD	TBD
		"	(d) Obtaining an exemption from organizational personnel with system maintenance responsibilities explicitly authorizing removal of the equipment from the facility.	Zero-cycle	P4	TBD	TBD	TBD
MA-4	MA-4	NONLOCAL MAINTENANCE	a. Approve and monitor nonlocal maintenance and diagnostic activities;	Zero-cycle	P3	TBD	TBD	TBD
		"	b. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system;	Zero-cycle	P3	TBD	TBD	TBD
		"	c. Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions;	Zero-cycle	P3	TBD	TBD	TBD
		"	d. Maintain records for nonlocal maintenance and diagnostic activities; and	Zero-cycle	P3	TBD	TBD	TBD
		"	e. Terminate session and network connections when nonlocal maintenance is completed.	Zero-cycle	P3	TBD	TBD	TBD
MA-5	MA-5	MAINTENANCE PERSONNEL	a. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel;	Zero-cycle	P3	TBD	TBD	TBD
		"	b. Verify that non-escorted personnel performing maintenance on the system possess the required access authorizations; and	Zero-cycle	P3	TBD	TBD	TBD
		"	c. Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.	Zero-cycle	P3	TBD	TBD	TBD
MA-6	MA-6	TIMELY MAINTENANCE	Obtain maintenance support and/or spare parts for critical system components that process, store, and transmit CJI within agency-defined recovery time and recovery point objectives of failure.	Zero-cycle	P3	TBD	TBD	TBD

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy: Media Protection (MP)								
5.8: MP-1	MP-1	Policy and Procedures	a. Develop, document, and disseminate to authorized individuals:	Existing	P2	Agency	Agency	Agency
		"	1. Agency-level media protection policy that:	Existing	P2	Agency	Agency	Agency
		"	(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance; and	Existing	P2	Agency	Agency	Agency
		"	(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and	Existing	P2	Agency	Agency	Agency
		"	2. Procedures to facilitate the implementation of the media protection policy and the associated media protection controls;	Existing	P2	Agency	Agency	Agency
		"	b. Designate an individual with security responsibilities to manage the development, documentation, and dissemination of the media protection policy and procedures; and	Existing	P2	Agency	Agency	Agency
		"	c. Review and update the current media protection:	Zero-cycle	P2	Agency	Agency	Agency
		"	1. Policy at least annually and following any security incidents involving digital and/or non-digital media; and	Zero-cycle	P2	Agency	Agency	Agency
		"	2. Procedures at least annually and following any security incidents involving digital and/or non-digital media.	Zero-cycle	P2	Agency	Agency	Agency
5.8: MP-2	MP-2	Media Access	Restrict access to digital and non-digital media to authorized individuals.	Existing	P2	Both	Both	Both
5.8: MP-3	MP-3	Media Marking	a. Mark system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and	Zero-cycle	P3	Both	Both	Both
		"	b. Exempt digital and non-digital media containing CJI from marking if the media remain within physically secure locations and controlled areas.	Zero-cycle	P3	Both	Both	Both
5.8: MP-4	MP-4	Media Storage	a. Physically control and securely store digital and non-digital media within physically secure locations or controlled areas and encrypt CJI on digital media when physical and personnel restrictions are not feasible; and	Existing	P2	Both	Both	Both
		"	b. Protect system media types defined in MP-4a until the media are destroyed or sanitized using approved equipment, techniques, and procedures.	Existing	P2	Both	Both	Both
5.8: MP-5	MP-5	Media Transport	a. Protect and control digital and non-digital media to help prevent compromise of the data during transport outside of the physically secure locations or controlled areas using encryption, as defined in Systems and Communications Protection (SC). Physical media will be protected at the same level as the information would be protected in electronic form. Restrict the activities associated with transport of electronic and physical media to authorized personnel;	Existing	P2	Agency	Both	Both
		"	b. Maintain accountability for system media during transport outside of the physically secure location or controlled areas;	Existing	P2	Both	Both	Both
		"	c. Document activities associated with the transport of system media; and	Existing	P2	Both	Both	Both
		"	d. Restrict the activities associated with the transport of system media to authorized personnel.	Existing	P2	Both	Both	Both
5.8: MP-6	MP-6	Media Sanitization	a. Sanitize or destroy digital and non-digital media prior to disposal, release out of agency control, or release for reuse using overwrite technology at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media will be destroyed (cut up, shredded, etc.). Physical media will be securely disposed of when no longer needed for investigative or security purposes, whichever is later. Physical media will be destroyed by crosscut shredding or incineration; and	Existing	P2	Agency	Both	Both

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
5.8: MP-6	MP-6	Media Sanitization (continued)	b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.	Existing	P2	Agency	Both	Both
5.8: MP-7	MP-7	Media Use	a. Restrict the use of digital and non-digital media on agency-owned systems that have been approved for use in the storage, processing, or transmission of criminal justice information by using technical, physical, or administrative controls (examples below); and	Existing	P2	Agency	Both	Both
		"	b. Prohibit the use of personally-owned digital media devices on all agency-owned or controlled systems that store, process, or transmit criminal justice information; and	Existing	P2	Agency	Both	Both
		"	c. Prohibit the use of digital media devices on all agency-owned or controlled systems that store, process, or transmit criminal justice information when such devices have no identifiable owner.	Existing	P2	Agency	Both	Both

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy: Physical and Environmental Protection (PE)								
PE-1	PE-1	POLICY AND PROCEDURES	a. Develop, document, and disseminate to organizational personnel with physical and environmental protection responsibilities:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. Agency-level physical and environmental protection policy that:	Zero-cycle	P2	TBD	TBD	TBD
		"	(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Zero-cycle	P2	TBD	TBD	TBD
		"	(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and	Zero-cycle	P2	TBD	TBD	TBD
		"	2. Procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental protection controls;	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Designate organizational personnel with information security responsibilities to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures; and	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Review and update the current physical and environmental protection:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. Policy annually and following any physical, environmental, or security related incidents involving CJI or systems used to process, store, or transmit CJI; and	Zero-cycle	P2	TBD	TBD	TBD
		"	2. Procedures annually and following any physical, environmental, or security related incidents involving CJI or systems used to process, store, or transmit CJI.	Zero-cycle	P2	TBD	TBD	TBD
PE-2	PE-2	PHYSICAL ACCESS AUTHORIZATIONS	a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides;	Existing	P2	Both	Both	Both
		"	b. Issue authorization credentials for facility access;	Existing	P2	Both	Both	Both
		"	c. Review the access list detailing authorized facility access by individuals annually and when personnel changes occur; and	Existing	P2	Both	Both	Both
		"	d. Remove individuals from the facility access list when access is no longer required.	Existing	P2	Both	Both	Both
PE-3	PE-3	PHYSICAL ACCESS CONTROL	a. Enforce physical access authorizations by:	Existing	P2	Both	Both	Both
		"	1. Verifying individual access authorizations before granting access to the facility; and	Existing	P2	Both	Both	Both
		"	2. Controlling ingress and egress to the facility using agency-implemented procedures and controls;	Existing	P2	Both	Both	Both
		"	b. Maintain physical access audit logs for the physically secure location and agency-defined sensitive areas;	Existing	P2	Both	Both	Both
		"	c. Control access to areas within the facility designated as non-publicly accessible by implementing physical access devices including, but not limited to keys, locks, combinations, biometric readers, placards, and/or card readers;	Existing	P2	Both	Both	Both
		"	d. Escort visitors and control visitor activity in all physically secure locations;	Existing	P2	Both	Both	Both
		"	e. Secure keys, combinations, and other physical access devices;	Existing	P2	Both	Both	Both
		"	f. Inventory all agency-issued physical access devices annually; and	Existing	P2	Both	Both	Both
		"	g. Change combinations and keys when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated.	Existing	P2	Both	Both	Both
PE-4	PE-4	ACCESS CONTROL FOR TRANSMISSION	Control physical access to information system distribution and transmission lines and devices within organizational facilities using agency-implemented procedures and controls.	Existing	P2	Both	Both	Both
		PE-5	PE-5	ACCESS CONTROL FOR OUTPUT DEVICES	Control physical access to output from monitors, printers, scanners, audio devices, facsimile machines, and copiers to prevent unauthorized individuals from obtaining the output.	Existing	P3	Both

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
PE-6	PE-6	MONITORING PHYSICAL ACCESS	a. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents;	Existing	P2	Both	Both	Both
		"	b. Review physical access logs quarterly and upon occurrence of any physical, environmental, or security-related incidents involving CJI or systems used to process, store, or transmit CJI; and	Existing	P2	Both	Both	Both
		"	c. Coordinate results of reviews and investigations with the organizational incident response capability.	Existing	P2	Both	Both	Both
PE-6 (1)	PE-6 (1)	(1) MONITORING PHYSICAL ACCESS INTRUSION ALARMS AND SURVEILLANCE EQUIPMENT	Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment.	Existing	P2	Both	Both	Both
PE-8	PE-8	VISITOR ACCESS RECORDS	a. Maintain visitor access records to the facility where the system resides for one (1) year;	Zero-cycle	P4	TBD	TBD	TBD
		"	b. Review visitor access records quarterly; and	Zero-cycle	P4	TBD	TBD	TBD
		"	c. Report anomalies in visitor access records to organizational personnel with physical and environmental protection responsibilities and organizational personnel with information security responsibilities.	Zero-cycle	P4	TBD	TBD	TBD
PE-8 (3)	PE-8 (3)	(3) VISITOR ACCESS RECORDS LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS	Limit personally identifiable information contained in visitor access records to the minimum PII necessary to achieve the purpose for which it is collected (see Section 4.3).	Zero-cycle	P4	TBD	TBD	TBD
		"	Note: Access to visitor access records is restricted to authorized agency personnel.	Zero-cycle	P4	TBD	TBD	TBD
PE-9	PE-9	POWER EQUIPMENT AND CABLING	Protect power equipment and power cabling for the system from damage and destruction.	Zero-cycle	P2	TBD	TBD	TBD
PE-10	PE-10	EMERGENCY SHUTOFF	a. Provide the capability of shutting off power to all information systems in emergency situations;	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Place emergency shutoff switches or devices in easily accessible locations to facilitate access for authorized personnel; and	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Protect emergency power shutoff capability from unauthorized activation.	Zero-cycle	P2	TBD	TBD	TBD
PE-11	PE-11	EMERGENCY POWER	Provide an uninterruptible power supply to facilitate an orderly shutdown of the information system or transition of the information system to an alternate power source in the event of a primary power source loss.	Zero-cycle	P2	TBD	TBD	TBD
PE-12	PE-12	EMERGENCY LIGHTING	Employ and maintain automatic emergency lighting for the system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.	Zero-cycle	P2	TBD	TBD	TBD
PE-13	PE-13	FIRE PROTECTION	Employ and maintain fire detection and suppression systems that are supported by an independent energy source.	Zero-cycle	P2	TBD	TBD	TBD
PE-13 (1)	PE-13 (1)	(1) FIRE PROTECTION DETECTION SYSTEMS — AUTOMATIC ACTIVATION AND NOTIFICATION	Employ fire detection systems that activate automatically and notify organizational personnel with physical and environmental protection responsibilities and police, fire, or emergency medical personnel in the event of a fire.	Zero-cycle	P2	TBD	TBD	TBD
PE-14	PE-14	ENVIRONMENTAL CONTROLS	a. Maintain adequate HVAC levels within the facility where the system resides at recommended system manufacturer levels; and	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Monitor environmental control levels continuously.	Zero-cycle	P2	TBD	TBD	TBD
PE-15	PE-15	WATER DAMAGE PROTECTION	Protect the system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.	Zero-cycle	P2	TBD	TBD	TBD

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
PE-16	PE-16	DELIVERY AND REMOVAL	a. Authorize and control information system-related components entering and exiting the facility; and	Existing	P3	Both	Both	Both
		"	b. Maintain records of the system components.	Existing	P3	Both	Both	Both
PE-17	PE-17	ALTERNATE WORK SITE	a. Determine and document all alternate facilities or locations allowed for use by employees;	Existing	P3	Both	Both	Both
		"	b. Employ the following controls at alternate work sites:	Existing	P3	Both	Both	Both
		"	1. Limit access to the area during CJI processing times to only those personnel authorized by the agency to access or view CJI.	Existing	P3	Both	Both	Both
		"	2. Lock the area, room, or storage container when unattended.	Existing	P3	Both	Both	Both
		"	3. Position information system devices and documents containing CJI in such a way as to prevent unauthorized individuals from access and view.	Existing	P3	Both	Both	Both
		"	4. Follow the encryption requirements found in SC-13 and SC-28 for electronic storage (i.e., data at-rest) of CJI.	Existing	P3	Both	Both	Both
		"	c. Assess the effectiveness of controls at alternate work sites; and	Existing	P3	Both	Both	Both
		"	d. Provide a means for employees to communicate with information security and privacy personnel in case of incidents.	Existing	P3	Both	Both	Both

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy: Planning (PL)								
PL-1	PL-1	POLICY AND PROCEDURES	a. Develop, document, and disseminate to organizational personnel with planning responsibilities:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. Agency-level planning policy that:	Zero-cycle	P2	TBD	TBD	TBD
		"	(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Zero-cycle	P2	TBD	TBD	TBD
		"	(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and	Zero-cycle	P2	TBD	TBD	TBD
		"	2. Procedures to facilitate the implementation of the planning policy and the associated planning controls;	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Designate organizational personnel with information security and privacy responsibilities to manage the development, documentation, and dissemination of the planning policy and procedures; and	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Review and update the current planning:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. Policy annually and following; any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI and	Zero-cycle	P2	TBD	TBD	TBD
		"	2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.	Zero-cycle	P2	TBD	TBD	TBD
PL-2	PL-2	SYSTEM SECURITY AND PRIVACY PLANS	a. Develop security and privacy plans for the system that:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. Are consistent with the organization’s enterprise architecture;	Zero-cycle	P2	TBD	TBD	TBD
		"	2. Explicitly define the constituent system components;	Zero-cycle	P2	TBD	TBD	TBD
		"	3. Describe the operational context of the system in terms of mission and business processes;	Zero-cycle	P2	TBD	TBD	TBD
		"	4. Identify the individuals that fulfill system roles and responsibilities;	Zero-cycle	P2	TBD	TBD	TBD
		"	5. Identify the information types processed, stored, and transmitted by the system;	Zero-cycle	P2	TBD	TBD	TBD
		"	6. Provide the security categorization of the system, including supporting rationale;	Zero-cycle	P2	TBD	TBD	TBD
		"	7. Describe any specific threats to the system that are of concern to the organization;	Zero-cycle	P2	TBD	TBD	TBD
		"	8. Provide the results of a privacy risk assessment for systems processing personally identifiable information;	Zero-cycle	P2	TBD	TBD	TBD
		"	9. Describe the operational environment for the system and any dependencies on or connections to other systems or system components;	Zero-cycle	P2	TBD	TBD	TBD
		"	10. Provide an overview of the security and privacy requirements for the system;	Zero-cycle	P2	TBD	TBD	TBD
		"	11. Identify any relevant control baselines or overlays, if applicable;	Zero-cycle	P2	TBD	TBD	TBD
		"	12. Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions;	Zero-cycle	P2	TBD	TBD	TBD
		"	13. Include risk determinations for security and privacy architecture and design decisions;	Zero-cycle	P2	TBD	TBD	TBD
		"	14. Include security- and privacy-related activities affecting the system that require planning and coordination with organizational personnel with system security and privacy planning and plan implementation responsibilities; system developers; organizational personnel with information security and privacy responsibilities; and	Zero-cycle	P2	TBD	TBD	TBD
		"	15. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation.	Zero-cycle	P2	TBD	TBD	TBD

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
PL-2	PL-2	SYSTEM SECURITY AND PRIVACY PLANS (continued)	b. Distribute copies of the plans and communicate subsequent changes to the plans to organizational personnel with system security and privacy planning and plan implementation responsibilities; system developers; organizational personnel with information security and privacy responsibilities;	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Review the system security and privacy plans at least annually or when required due to system changes or modifications;	Zero-cycle	P2	TBD	TBD	TBD
		"	d. Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments; and	Zero-cycle	P2	TBD	TBD	TBD
		"	e. Protect the plans from unauthorized disclosure and modification.	Zero-cycle	P2	TBD	TBD	TBD
PL-4	PL-4	RULES OF BEHAVIOR	a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy;	Zero-cycle	P3	TBD	TBD	TBD
		"	b. Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system;	Zero-cycle	P3	TBD	TBD	TBD
		"	c. Review and update the rules of behavior at least annually; and	Zero-cycle	P3	TBD	TBD	TBD
		"	d. Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge annually, or when the rules are revised or updated.	Zero-cycle	P3	TBD	TBD	TBD
PL-4 (1)	PL-4 (1)	(1) RULES OF BEHAVIOR SOCIAL MEDIA AND EXTERNAL SITE/APPLICATION USAGE RESTRICTIONS	Include in the rules of behavior, restrictions on:	Zero-cycle	P3	TBD	TBD	TBD
		"	(a) Use of social media, social networking sites, and external sites/applications;	Zero-cycle	P3	TBD	TBD	TBD
		"	(b) Posting organizational information on public websites; and	Zero-cycle	P3	TBD	TBD	TBD
		"	(c) Use of organization-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications.	Zero-cycle	P3	TBD	TBD	TBD
PL-8	PL-8	SECURITY AND PRIVACY ARCHITECTURES	a. Develop security and privacy architectures for the system that:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information;	Zero-cycle	P2	TBD	TBD	TBD
		"	2. Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals;	Zero-cycle	P2	TBD	TBD	TBD
		"	3. Describe how the architectures are integrated into and support the enterprise architecture; and	Zero-cycle	P2	TBD	TBD	TBD
		"	4. Describe any assumptions about, and dependencies on, external systems and services;	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Review and update the architectures at least annually or when changes to the system or its environment occur to reflect changes in the enterprise architecture; and	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and acquisitions.	Zero-cycle	P2	TBD	TBD	TBD
PL-9	PL-9	CENTRAL MANAGEMENT	The CJISSECPOL is centrally managed by the FBI CJIS ISO.	Zero-cycle	P4	TBD	TBD	TBD
PL-10	PL-10	BASELINE SELECTION	Select a control baseline for the system.	Zero-cycle	P3	TBD	TBD	TBD
PL-11	PL-11	BASELINE TAILORING	Tailor the selected control baseline by applying specified tailoring actions.	Zero-cycle	P3	TBD	TBD	TBD

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy Section: Personnel Security (PS)								
	PS-1	POLICY AND PROCEDURES	a. Develop, document, and disseminate to organizational personnel with personnel security responsibilities:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. Agency-level personnel security policy that:	Zero-cycle	P2	TBD	TBD	TBD
		"	a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and	Zero-cycle	P2	TBD	TBD	TBD
		"	2. Procedures to facilitate the implementation of the personnel security policy and the associated personnel security controls;	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Designate organizational personnel with information security responsibilities to manage the development, documentation, and dissemination of the personnel security policy and procedures; and	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Review and update the current personnel security:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. Policy annually and following assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and	Zero-cycle	P2	TBD	TBD	TBD
		"	2. Procedures annually and following assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.	Zero-cycle	P2	TBD	TBD	TBD
	PS-2	POSITION RISK DESIGNATION	a. Assign a risk designation to all organizational positions;	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Establish screening criteria for individuals filling those positions; and	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Review and update position risk designations as required.	Zero-cycle	P2	TBD	TBD	TBD
5.12.1	PS-3	PERSONNEL SCREENING	a. Screen individuals prior to authorizing access to the information system;	Existing	P2	Agency	Agency	Agency
		"	1. To properly screen, state of residency and national fingerprint-based record checks shall be conducted. National fingerprint-based record checks must be conducted pursuant to an FBI approved authority such as a federal statute or a state statute approved pursuant to Public Law 92-544. If the person resides in a different state than that of the assigned agency, the agency shall also conduct state (of the agency) record checks. When appropriate, the screening shall be consistent with:	Existing	P2	Agency	Agency	Agency
		"	a. 5 CFR 731.106; and/or	Existing	P2	Agency	Agency	Agency
		"	b. Office of Personnel Management policy, regulations, and guidance; and/or	Existing	P2	Agency	Agency	Agency
		"	c. agency policy, regulations, and guidance.	Existing	P2	Agency	Agency	Agency
		"	Agencies authorized to bypass state repositories in compliance with federal law must only conduct a national fingerprint-based record check.	Existing	P2	Agency	Agency	Agency
		"	Agencies without approved statutory authority authorizing or requiring civil fingerprint-based record checks on personnel with access to CHRI are exempt from this requirement until such time as appropriate statutory authority is obtained to conduct such record checks.	Existing	P2	Agency	Agency	Agency
		"	2. All requests for access shall be made as specified by the CSO, Authorized Recipient Official, or IA Official. The CSO/designee, Authorized Recipient Official/designee, or IA Official is authorized to approve access to CJI. All CSO designees shall be from an authorized criminal justice agency. All Authorized Recipient designees shall be employed by the Authorized Recipient Agency.	Existing	P2	Agency	Agency	Agency
		"	3. If a criminal history record of any kind exists, access to CJI shall not be granted until the CSO/designee, Authorized Recipient Official/designee, or IA Official reviews the matter to determine if access is appropriate.	Existing	P2	Agency	Agency	Agency

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
5.12.1	PS-3	PERSONNEL SCREENING (continued)	a. If a felony conviction of any kind exists, the agency shall deny access to CJI. However, the requesting agency may ask for a review by the CSO/designee, Authorized Recipient Official/designee, or IA Official in extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance.	Existing	P2	Agency	Agency	Agency
		"	b. Applicants with a record of misdemeanor offense(s) may be granted access if the CSO/designee, Authorized Recipient Official/designee, or IA Official, determines the nature or severity of the misdemeanor offense(s) do not warrant disqualification. The requesting agency may request the CSO/designee, Authorized Recipient	Existing	P2	Agency	Agency	Agency
		"	c. If a criminal history record of any kind is found on a contractor, the CA shall be formally notified of continuing fitness determination and system access shall be delayed pending review of the criminal history record information. The CA shall in turn notify the contractor's security officer.	Existing	P2	Agency	Agency	Agency
		"	4. If the person appears to be a fugitive or has an arrest history without conviction, the CSO/designee, Authorized Recipient Official/designee, or IA Official shall review the matter to determine if access to CJI is appropriate.	Existing	P2	Agency	Agency	Agency
		"	5. If the person already has access to CJI and is subsequently arrested and or convicted, continued access to CJI shall be determined by the CSO/designee, Authorized Recipient Official/designee, or IA Official. This does not implicitly grant hiring/firing authority with the CSA, Authorized Recipient, or IA Official only the authority to grant access to CJI. For offenses other than felonies, the CSO/designee, Authorized Recipient Official/designee, or IA Official has the latitude to delegate continued access determinations.	Existing	P2	Agency	Agency	Agency
		"	6. If the CSO/designee, Authorized Recipient Official/designee, or IA Official determines that access to CJI by the person would not be in the public interest, access shall be denied and the person's appointing authority shall be notified in writing of the access denial.	Existing	P2	Agency	Agency	Agency
		"	7. The criminal and non-criminal justice agency shall maintain a list of personnel who have been authorized unescorted access to unencrypted CJI and shall, upon request, provide a current copy of the access list to the CSO/designee, Authorized Recipient Official/designee, or IA Official.	Existing	P2	Agency	Agency	Agency
		"	and	Existing	P2	Agency	Agency	Agency
		"	b. Recommend rescreening individuals in accordance with PS-3(a)(1) above. The authority authorized for the national fingerprint-based background check must also authorize the rescreening.	Existing	P2	Agency	Agency	Agency
	PS-4	PERSONNEL TERMINATION	Upon termination of individual employment:	Zero-cycle	P2	TBD	TBD	TBD
		"	a. Disable system access within twenty-four (24) hours;	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Terminate or revoke any authenticators and credentials associated with the individual;	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Conduct exit interviews that include a discussion of non-disclosure of CJI and PII;	Zero-cycle	P2	TBD	TBD	TBD
		"	d. Retrieve all security-related organizational system-related property; and	Zero-cycle	P2	TBD	TBD	TBD
		"	e. Retain access to organizational information and systems formerly controlled by terminated individual.	Zero-cycle	P2	TBD	TBD	TBD

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
5.12.3	PS-5	PERSONNEL TRANSFER	a. Review and confirm ongoing operational need for current logical and physical access authorizations to systems and facilities when individuals are reassigned or transferred to other positions within the organization;	Existing	P3	Both	Both	Both
		"	b. Initiate appropriate actions such as closing and establishing accounts and changing system access authorizations within twenty-four (24) hours;	Existing	P3	Both	Both	Both
		"	c. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and	Existing	P3	Both	Both	Both
		"	d. Notify organizational personnel with information security responsibilities, organizational personnel with personnel security responsibilities, system/network administrators, and organizational personnel with account management responsibilities-prior to personnel transfer.	Existing	P3	Both	Both	Both
	PS-6	ACCESS AGREEMENTS	a. Develop and document access agreements for organizational systems;	Zero-cycle	P4	TBD	TBD	TBD
		"	b. Review and update the access agreements at least annually; and	Zero-cycle	P4	TBD	TBD	TBD
		"	c. Verify that individuals requiring access to organizational information and systems:	Zero-cycle	P4	TBD	TBD	TBD
		"	1. Sign appropriate access agreements prior to being granted access; and	Zero-cycle	P4	TBD	TBD	TBD
		"	2. Re-sign access agreements to maintain access to organizational systems when access agreements have been updated or when signatories change.	Zero-cycle	P4	TBD	TBD	TBD
5.12.2	PS-7	EXTERNAL PERSONNEL SECURITY	a. Establish personnel security requirements, including security roles and responsibilities for external providers;	Existing	P2	Agency	Agency	Agency
		"	b. Require external providers to comply with personnel security policies and procedures established by the organization;	Existing	P2	Agency	Agency	Agency
		"	c. Document personnel security requirements;	Existing	P2	Agency	Agency	Agency
		"	d. Require external providers to notify organizational personnel with information security responsibilities, organizational personnel with personnel security responsibilities, system/network administrators, or organizational personnel with account management responsibilities of any personnel transfers or terminations of external personnel who possess organizational credentials and/or badges, or who have system privileges within twenty-four (24) hours; and	Existing	P2	Both	Both	Both
		"	e. Monitor provider compliance with personnel security requirements.	Existing	P2	Agency	Agency	Agency
	PS-8	PERSONNEL SANCTIONS	a. Employ a formal sanctions process for individuals failing to comply with established information security and privacy policies and procedures; and	Zero-cycle	P4	TBD	TBD	TBD
		"	b. Notify organizational personnel with information security responsibilities, organizational personnel with personnel security responsibilities, system/network administrators, or organizational personnel with account management responsibilities within twenty-four (24) hours when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.	Zero-cycle	P4	TBD	TBD	TBD
	PS-9	POSITION DESCRIPTIONS	Incorporate security and privacy roles and responsibilities into organizational position descriptions.	Zero-cycle	P4	TBD	TBD	TBD

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy: Risk Assessment (RA)								
RA-1	RA-1	POLICY AND PROCEDURES	a. Develop, document, and disseminate to organizational personnel with risk assessment responsibilities:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. Agency Level risk assessment policy that:	Zero-cycle	P2	TBD	TBD	TBD
		"	(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Zero-cycle	P2	TBD	TBD	TBD
		"	(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and	Zero-cycle	P2	TBD	TBD	TBD
		"	2. Procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls;	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Designate organizational personnel with security and privacy responsibilities to manage the development, documentation, and dissemination of the risk assessment policy and procedures; and	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Review and update the current risk assessment:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. Policy annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI; and	Zero-cycle	P2	TBD	TBD	TBD
		"	2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.	Zero-cycle	P2	TBD	TBD	TBD
RA-2	RA-2	SECURITY CATEGORIZATION	a. Categorize the system and information it processes, stores, and transmits;	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Document the security categorization results, including supporting rationale, in the security plan for the system; and	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Verify that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.	Zero-cycle	P2	TBD	TBD	TBD
RA-3	RA-3	RISK ASSESSMENT	a. Conduct a risk assessment, including:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. Identifying threats to and vulnerabilities in the system;	Zero-cycle	P2	TBD	TBD	TBD
		"	2. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and	Zero-cycle	P2	TBD	TBD	TBD
		"	3. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information;	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments;	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Document risk assessment results in risk assessment report;	Zero-cycle	P2	TBD	TBD	TBD
		"	d. Review risk assessment results at least quarterly;	Zero-cycle	P2	TBD	TBD	TBD
		"	e. Disseminate risk assessment results to organizational personnel with risk assessment responsibilities and organizational personnel with security and privacy responsibilities; and	Zero-cycle	P2	TBD	TBD	TBD
		"	f. Update the risk assessment at least quarterly or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.	Zero-cycle	P2	TBD	TBD	TBD
RA-5	RA-5	VULNERABILITY MONITORING AND SCANNING	a. Monitor and scan for vulnerabilities in the system and hosted applications at least monthly and when new vulnerabilities potentially affecting the system are identified and reported;	10/1/2024	P1	TBD	TBD	TBD
		"	b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:	10/1/2024	P1	TBD	TBD	TBD
		"	1. Enumerating platforms, software flaws, and improper configurations;	10/1/2024	P1	TBD	TBD	TBD
		"	2. Formatting checklists and test procedures; and	10/1/2024	P1	TBD	TBD	TBD
		"	3. Measuring vulnerability impact;	10/1/2024	P1	TBD	TBD	TBD

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
RA-5	RA-5	VULNERABILITY MONITORING AND SCANNING (continued)	c. Analyze vulnerability scan reports and results from vulnerability monitoring;	10/1/2024	P1	TBD	TBD	TBD
		"	d. Remediate legitimate vulnerabilities within the number of days listed;	10/1/2024	P1	TBD	TBD	TBD
		"	• Critical–15 days	10/1/2024	P1	TBD	TBD	TBD
		"	• High–30 days	10/1/2024	P1	TBD	TBD	TBD
		"	• Medium–60 days	10/1/2024	P1	TBD	TBD	TBD
		"	• Low–90 days; and	10/1/2024	P1	TBD	TBD	TBD
		"	e. Share information obtained from the vulnerability monitoring process and control assessments with organizational personnel with risk assessment, control assessment, and vulnerability scanning responsibilities to help eliminate similar vulnerabilities in other systems; and	10/1/2024	P1	TBD	TBD	TBD
		"	f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.	10/1/2024	P1	TBD	TBD	TBD
RA-5 (2)	RA-5 (2)	(2) VULNERABILITY MONITORING AND SCANNING UPDATE VULNERABILITIES TO BE SCANNED	Update the system vulnerabilities to be scanned within 24 hours prior to running a new scan or when new vulnerabilities are identified and reported.	10/1/2024	P1	TBD	TBD	TBD
RA-5 (5)	RA-5 (5)	(5) VULNERABILITY MONITORING AND SCANNING PRIVILEGED ACCESS	Implement privileged access authorization to information system components containing or processing CJI for vulnerability scanning activities requiring privileged access.	10/1/2024	P1	TBD	TBD	TBD
RA-5 (11)	RA-5 (11)	(11) VULNERABILITY MONITORING AND SCANNING PUBLIC DISCLOSURE PROGRAM	Establish a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components.	10/1/2024	P1	TBD	TBD	TBD
RA-7	RA-7	RISK RESPONSE	Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.	Zero-cycle	P2	TBD	TBD	TBD
RA-9	RA-9	CRITICALITY ANALYSIS	Identify critical system components and functions by performing a criticality analysis for information system components containing or processing CJI at the planning, design, development, testing, implementation, and maintenance stages of the system development life cycle.	Zero-cycle	P2	TBD	TBD	TBD

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy: System and Services Acquisition (SA)								
	SA-1	POLICY AND PROCEDURES	a. Develop, document, and disseminate to: organizational personnel with system and services acquisition responsibilities; organizational personnel with information security and privacy responsibilities; organizational personnel with supply chain risk management responsibilities:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. Agency/Entity information systems and services acquisition policy for systems that used to process, store, or transmit CJI that:	Zero-cycle	P2	TBD	TBD	TBD
		"	(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Zero-cycle	P2	TBD	TBD	TBD
		"	(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and	Zero-cycle	P2	TBD	TBD	TBD
		"	2. Procedures to facilitate the implementation of the system and services acquisition policy and the associated system and services acquisition controls;	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Designate organizational personnel with information security responsibilities and organizational personnel with system and services acquisition responsibilities to manage the development, documentation, and dissemination of the system and services acquisition policy and procedures; and	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Review and update the current system and services acquisition:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. Policy following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI; and	Zero-cycle	P2	TBD	TBD	TBD
		"	2. Procedures following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.	Zero-cycle	P2	TBD	TBD	TBD
	SA-2	ALLOCATION OF RESOURCES	a. Determine the high-level information security and privacy requirements for the system or system service in mission and business process planning;	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Determine, document, and allocate the resources required to protect the system or system service as part of the organizational capital planning and investment control process; and	Zero-cycle	P2	TBD	TBD	TBD
	SA-3	SYSTEM DEVELOPMENT LIFE CYCLE	a. Acquire, develop, and manage the system using an agency documented system development lifecycle process that incorporates information security and privacy considerations;	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Define and document information security and privacy roles and responsibilities throughout the system development life cycle;	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Identify individuals having information security and privacy roles and responsibilities; and	Zero-cycle	P2	TBD	TBD	TBD
		"	d. Integrate the organizational information security and privacy risk management process into system development life cycle activities.	Zero-cycle	P2	TBD	TBD	TBD
	SA-4	ACQUISITION PROCESS	Include the following requirements, descriptions, and criteria, explicitly or by reference, using agency defined contract language in the acquisition contract for the system, system component, or system service:	Zero-cycle	P2	TBD	TBD	TBD
		"	a. Security and privacy functional requirements;	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Strength of mechanism requirements;	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Security and privacy assurance requirements;	Zero-cycle	P2	TBD	TBD	TBD
		"	d. Controls needed to satisfy the security and privacy requirements.	Zero-cycle	P2	TBD	TBD	TBD
		"	e. Security and privacy documentation requirements;	Zero-cycle	P2	TBD	TBD	TBD
		"	f. Requirements for protecting security and privacy documentation;	Zero-cycle	P2	TBD	TBD	TBD
		"	g. Description of the system development environment and environment in which the system is intended to operate;	Zero-cycle	P2	TBD	TBD	TBD
		"	h. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; and	Zero-cycle	P2	TBD	TBD	TBD
	"	i. Acceptance criteria.	Zero-cycle	P2	TBD	TBD	TBD	
	SA-4(1)	(1) ACQUISITION PROCESS FUNCTIONAL PROPERTIES OF CONTROLS	Require the developer of the system, system component, or system service to provide a description of the functional properties of the controls to be implemented.	Zero-cycle	P2	TBD	TBD	TBD

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
	SA-4(2)	(2) ACQUISITION PROCESS DESIGN AND IMPLEMENTATION INFORMATION FOR CONTROLS	Require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes: security-relevant external system interfaces; high-level design at and a project plan that addresses sufficient detail to permit analysis and testing of the controls.	Zero-cycle	P2	TBD	TBD	TBD
	SA-4(9)	(9) ACQUISITION PROCESS FUNCTIONS, PORTS, PROTOCOLS, AND SERVICES IN USE	Require the developer of the system, system component, or system service to identify the functions, ports, protocols, and services intended for organizational use.	Zero-cycle	P2	TBD	TBD	TBD
	SA-4(10)	(10) ACQUISITION PROCESS USE OF APPROVED PIV PRODUCTS	Employ only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational systems.	Zero-cycle	P2	TBD	TBD	TBD
	SA-5	SYSTEM DOCUMENTATION	a. Obtain or develop administrator documentation for the system, system component, or system service that describes:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. Secure configuration, installation, and operation of the system, component, or service;	Zero-cycle	P2	TBD	TBD	TBD
		"	2. Effective use and maintenance of security and privacy functions and mechanisms; and	Zero-cycle	P2	TBD	TBD	TBD
		"	3. Known vulnerabilities regarding configuration and use of administrative or privileged functions;	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Obtain or develop user documentation for the system, system component, or system service that describes:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. User-accessible security and privacy functions and mechanisms and how to effectively use those functions and mechanisms;	Zero-cycle	P2	TBD	TBD	TBD
		"	2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner and protect individual privacy; and	Zero-cycle	P2	TBD	TBD	TBD
		"	3. User responsibilities in maintaining the security of the system, component, or service and privacy of individuals;	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Document steps to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent by contacting manufacturers, suppliers, or developers and conducting web-based searches in response; and	Zero-cycle	P2	TBD	TBD	TBD
		"	d. Distribute documentation to organizational personnel with system and services responsibilities.	Zero-cycle	P2	TBD	TBD	TBD
	SA-8	SECURITY AND PRIVACY ENGINEERING PRINCIPLES	Apply agency documented systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components.	Zero-cycle	P2	TBD	TBD	TBD
	SA-8(33)	(33) SECURITY AND PRIVACY ENGINEERING PRINCIPLES MINIMIZATION	Implement the privacy principle of minimization using only the Personally Identifiable Information necessary to perform system engineering.	Zero-cycle	P2	TBD	TBD	TBD
	SA-9	EXTERNAL SYSTEM SERVICES	a. Require that providers of external system services comply with organizational security and privacy requirements and employ system and services acquisition security controls in accordance with the CJISSECPOL including the following agreements when applicable:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. Management control agreement: A NCJA (government) designated to perform criminal justice functions for a CJA shall be eligible for access to the CJI. Access shall be permitted when such designation is authorized pursuant to executive order, statute, regulation, or interagency agreement. The NCJA shall sign and execute a management control agreement (MCA) with the CJA stipulating management control of the criminal justice function remains solely with the CJA. An example of an NCJA (government) is a city information technology (IT) department. An example of an MCA is provided in Appendix D.2.	Zero-cycle	P2	TBD	TBD	TBD

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
	SA-9	EXTERNAL SYSTEM SERVICES (continued)	2. Security Addendum: The CJIS Security Addendum is a uniform addendum to an agreement between the government agency and a private contractor, approved by the Director of the FBI, acting for the U.S. Attorney General, as referenced in Title 28 CFR 20.33 (a)(7), which specifically authorizes access to CHRI, limits the use of the information to the purposes for which it is provided, ensures the security and confidentiality of the information is consistent with existing regulations and the CJISSECPOL, provides for sanctions, and contains such other provisions as the Attorney General may require.	Zero-cycle	P2	TBD	TBD	TBD
		"	Private contractors designated to:	Zero-cycle	P2	TBD	TBD	TBD
		"	a. Perform criminal justice functions for a CJA; or	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Perform criminal justice dispatching functions or data processing/information services for a NCJA (government), shall be eligible for access to CJI pursuant to an agreement which specifically identifies the private contractor's purpose and scope of providing services for the administration of criminal justice. The agreement between the CJA/NCJA and the private contractor shall incorporate the CJISSECPOL.	Zero-cycle	P2	TBD	TBD	TBD
		"	Private contractors who perform criminal justice functions shall meet the same training and certification criteria required by governmental agencies performing a similar function and shall be subject to the same extent of audit review as are local user agencies. All private contractors who perform criminal justice functions shall acknowledge, via signing of the CJIS Security Addendum Certification page (page H- 8), compliance with all aspects of the CJIS Security Addendum. The CJIS Security Addendum is presented in Appendix H (pages H-6 and 7). Modifications to the CJIS Security Addendum shall be enacted only by the FBI.	Zero-cycle	P2	TBD	TBD	TBD
		"	3. Outsourcing Standards for Channelers: Channelers designated to request civil fingerprint-based background checks on behalf of a NCJA (public) or NCJA (private) for noncriminal justice functions shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. All Channelers accessing CJI shall be subject to the terms and conditions described in the Compact Council Security and Management Control Outsourcing Standard. Each Channeler that directly accesses CJI shall also allow the FBI to conduct periodic penetration testing. Channelers leveraging CJI to perform civil functions on behalf of an Authorized Recipient shall meet the same training and certification criteria required by governmental agencies performing a similar function and shall be subject to the same extent of audit review as are local user agencies.	Zero-cycle	P2	TBD	TBD	TBD
		"	4. Outsourcing Standards for Non-Channelers: Contractors designated to perform noncriminal justice ancillary functions on behalf of a NCJA (public) or NCJA (private) for noncriminal justice functions shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. All contractors accessing CJI shall be subject to the terms and conditions described in the Compact Council Outsourcing Standard for Non-Channelers. Contractors leveraging CJI to perform civil functions on behalf of an Authorized Recipient shall meet the same training and certification criteria required by governmental agencies performing a similar function and shall be subject to the same extent of audit review as are local user agencies.	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Define and document organizational oversight and user roles and responsibilities with regard to external system services; and	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Employ the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. All agencies having access to CJI shall permit an inspection team to conduct an appropriate inquiry and audit of any alleged security violations.	Zero-cycle	P2	TBD	TBD	TBD

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
	SA-9	EXTERNAL SYSTEM SERVICES (continued)	2. At a minimum, triennially audit all external service providers which have access to the information system in order to ensure compliance with applicable statutes, regulations, and policies.	Zero-cycle	P2	TBD	TBD	TBD
		"	3. Have the authority to conduct unannounced security inspections and scheduled audits of external service providers facilities.	Zero-cycle	P2	TBD	TBD	TBD
		"	4. Have the authority, on behalf of another CSA, to conduct a CJISSECPOL compliance audit of contractor facilities and provide the results to the requesting CSA. If a subsequent CSA requests an audit of the same contractor facility, the CSA may provide the results of the previous audit unless otherwise notified by the requesting CSA that a new audit be performed.	Zero-cycle	P2	TBD	TBD	TBD
		"	Note: Compliance audit requirements are outlined in the Security and Management Control Outsourcing Standard for Non-Channeler and Channeling related to outsourcing noncriminal justice administrative functions.	Zero-cycle	P2	TBD	TBD	TBD
	SA-9(2)	(2) EXTERNAL SYSTEM SERVICES IDENTIFICATION OF FUNCTIONS, PORTS, PROTOCOLS, AND SERVICES	Require providers of the following external system services to identify the functions, ports, protocols, and other services required for the use of such services: any system with a local, network, or remote connection to an agency information system.	Zero-cycle	P2	TBD	TBD	TBD
	SA-10	DEVELOPER CONFIGURATION MANAGEMENT	Require the developer of the system, system component, or system service to:	Zero-cycle	P2	TBD	TBD	TBD
		"	a. Perform configuration management during system, component, or service during design, development, implementation, operation, and disposal;	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Document, manage, and control the integrity of changes to security configuration, network diagrams, and system components (hardware, software, firmware) by implementing access restrictions such as least privilege for changes;	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Implement only organization-approved changes to the system, component, or service;	Zero-cycle	P2	TBD	TBD	TBD
		"	d. Document approved changes to the system, component, or service and the potential security and privacy impacts of such changes; and	Zero-cycle	P2	TBD	TBD	TBD
		"	e. Track security flaws and flaw resolution within the system, component, or service and report findings to the individual(s) with information security responsibilities and an individual(s) with system and services acquisition responsibilities.	Zero-cycle	P2	TBD	TBD	TBD
	SA-11	DEVELOPER TESTING AND EVALUATION	Require the developer of the system, system component, or system service, at all post-design stages of the system development life cycle, to:	Zero-cycle	P2	TBD	TBD	TBD
		"	a. Develop and implement a plan for ongoing security and privacy control assessments;	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Perform system and regression testing/evaluation at a level of comprehensive testing;	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Produce evidence of the execution of the assessment plan and the results of the testing and evaluation;	Zero-cycle	P2	TBD	TBD	TBD
		"	d. Implement a verifiable flaw remediation process; and	Zero-cycle	P2	TBD	TBD	TBD
		"	e. Correct flaws identified during testing and evaluation.	Zero-cycle	P2	TBD	TBD	TBD

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
	SA-15	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS	a. Require the developer of the system, system component, or system service to follow a documented development process that:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. Explicitly addresses security and privacy requirements;	Zero-cycle	P2	TBD	TBD	TBD
		"	2. Identifies the standards and tools used in the development process;	Zero-cycle	P2	TBD	TBD	TBD
		"	3. Documents the specific tool options and tool configurations used in the development process; and	Zero-cycle	P2	TBD	TBD	TBD
		"	4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Review the development process, standards, tools, tool options, and tool configurations to determine if the process, standards, tools, tool options and tool configurations selected and employed can satisfy security and privacy requirements during design, development, implementation, operation, and disposal.	Zero-cycle	P2	TBD	TBD	TBD
	SA-15(1)	(1) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS CRITICALITY ANALYSIS	Require the developer of the system, system component, or system service to perform a criticality analysis:	Zero-cycle	P3	TBD	TBD	TBD
		"	a. At the following decision points in the system development life cycle: design, development, implementation, and operational; and	Zero-cycle	P3	TBD	TBD	TBD
		"	b. At the following level of rigor: comprehensive testing.	Zero-cycle	P3	TBD	TBD	TBD
5.14: SA-22	SA-22	UNSUPPORTED SYSTEM COMPONENTS	a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or	Zero-cycle	P2	Both	Both	Both
		"	b. Provide the following option for alternative sources for continued support for unsupported components: original manufacturer support, or original contracted vendor support.	Zero-cycle	P2	Both	Both	Both

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy: Systems and Communications Protection (SC)								
SC-1	SC-1	POLICY AND PROCEDURES	a. Develop, document, and disseminate to organizational personnel with system and communications protection responsibilities:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. Agency-level system and communications protection policy that:	Zero-cycle	P2	TBD	TBD	TBD
		"	(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Zero-cycle	P2	TBD	TBD	TBD
		"	(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and	Zero-cycle	P2	TBD	TBD	TBD
		"	2. Procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls;	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Designate organizational personnel with information security responsibilities to manage the development, documentation, and dissemination of the system and communications protection policy and procedures; and	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Review and update the current system and communications protection:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. Policy annually and following any changes and security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI; and	Zero-cycle	P2	TBD	TBD	TBD
		"	2. Procedures annually and following any changes and security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.	Zero-cycle	P2	TBD	TBD	TBD
SC-2	SC-2	SEPARATION OF SYSTEM AND USER FUNCTIONALITY	Separate user functionality, including user interface services, from system management functionality.	Existing	P2	Both	Service Provider	Service Provider
SC-4	SC-4	INFORMATION IN SHARED SYSTEM RESOURCES	Prevent unauthorized and unintended information transfer via shared system resources.	Existing	P2	TBD	TBD	TBD
SC-5	SC-5	DENIAL-OF-SERVICE PROTECTION	a. Protect against or limit the effects of the following types of denial-of-service events: distributed denial of service, DNS Denial of Service, etc.; and	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Employ the following controls to achieve the denial-of-service objective: boundary protection devices and intrusion detection or prevention devices.	Zero-cycle	P2	TBD	TBD	TBD
SC-7	SC-7	BOUNDARY PROTECTION	a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system;	Existing	P1	Both	Service Provider	Service Provider
		"	b. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal organizational networks; and	Existing	P1	Both	Service Provider	Service Provider
		"	c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.	Existing	P1	Both	Service Provider	Service Provider
SC-7 (3)	SC-7 (3)	BOUNDARY PROTECTION ACCESS POINTS	Limit the number of external network connections to the system.	10/1/2024	P1	TBD	TBD	TBD
SC-7 (4)	SC-7 (4)	BOUNDARY PROTECTION EXTERNAL TELECOMMUNICATIONS SERVICES	(a) Implement a managed interface for each external telecommunication service;	10/1/2024	P1	TBD	TBD	TBD
		"	(b) Establish a traffic flow policy for each managed interface;	10/1/2024	P1	TBD	TBD	TBD
		"	(c) Protect the confidentiality and integrity of the information being transmitted across each interface;	10/1/2024	P1	TBD	TBD	TBD
		"	(d) Document each exception to the traffic flow policy with a supporting mission or business need and duration of that need;	10/1/2024	P1	TBD	TBD	TBD

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
SC-7 (4)	SC-7 (4)	BOUNDARY PROTECTION EXTERNAL TELECOMMUNICATIONS SERVICES (continued)	(e) Review exceptions to the traffic flow policy annually, after any incident, and after any major changes impacting the information system, while remove exceptions that are no longer supported by an explicit mission or business need;	10/1/2024	P1	TBD	TBD	TBD
		"	(f) Prevent unauthorized exchange of control plane traffic with external networks;	10/1/2024	P1	TBD	TBD	TBD
		"	(g) Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks; and	10/1/2024	P1	TBD	TBD	TBD
		"	(h) Filter unauthorized control plane traffic from external networks.	10/1/2024	P1	TBD	TBD	TBD
SC-7 (5)	SC-7 (5)	BOUNDARY PROTECTION DENY BY DEFAULT — ALLOW BY EXCEPTION	Deny network communications traffic by default and allow network communications traffic by exception at boundary devices for information systems used to process, store, or transmit CJI.	10/1/2024	P1	TBD	TBD	TBD
SC-7 (7)	SC-7 (7)	BOUNDARY PROTECTION SPLIT TUNNELING FOR REMOTE DEVICES	Prevent split tunneling for remote devices connecting to organizational systems.	10/1/2024	P1	TBD	TBD	TBD
SC-7 (8)	SC-7 (8)	BOUNDARY PROTECTION ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS	Route all internal communications traffic that may be proxied, except traffic specifically exempted by organizational personnel with information security responsibilities, to all untrusted networks through authenticated proxy servers at managed interfaces.	Existing	P1	Both	Service Provider	Service Provider
SC-7 (24)	SC-7 (24)	BOUNDARY PROTECTION PERSONALLY IDENTIFIABLE INFORMATION	For systems that process personally identifiable information:	10/1/2024	P1	TBD	TBD	TBD
		"	(a) Apply the following processing rules to data elements of personally identifiable information: all applicable laws, executive orders, directives, regulations, policies, standards, and guidelines;	10/1/2024	P1	TBD	TBD	TBD
		"	(b) Monitor for permitted processing at the external interfaces to the system and at key internal boundaries within the system;	10/1/2024	P1	TBD	TBD	TBD
		"	(c) Document each processing exception; and	10/1/2024	P1	TBD	TBD	TBD
		"	(d) Review and remove exceptions that are no longer supported.	10/1/2024	P1	TBD	TBD	TBD
SC-8	SC-8	TRANSMISSION CONFIDENTIALITY AND INTEGRITY	Protect the confidentiality and integrity of transmitted information.	Existing	P2	Both	Service Provider	Service Provider
		"	Metadata derived from unencrypted CJI shall be protected in the same manner as CJI and shall not be used for any advertising or other commercial purposes by any cloud service provider or other associated entity.	Existing	P2	Service Provider	Service Provider	Service Provider
SC-8 (1)	SC-8 (1)	TRANSMISSION CONFIDENTIALITY AND INTEGRITY CRYPTOGRAPHIC PROTECTION	Implement cryptographic mechanisms to prevent unauthorized disclosure and detect unauthorized changes or access to CJI during transmission.	Existing	P2	Both	Service Provider	Service Provider
SC-10	SC-10	NETWORK DISCONNECT	Terminate the network connection associated with a communications session at the end of the session or after one (1) hour of inactivity.	Zero-cycle	P3	TBD	TBD	TBD
		"	NOTE: In the interest of safety, devices that are: (1) part of a criminal justice conveyance; or (2) used to perform dispatch functions and located within a physically secure location; or (3) terminals designated solely for the purpose of receiving alert notifications (i.e., receive only terminals or ROT) and used within physically secure location facilities that remain staffed when in operation, are exempt from this requirement.	Zero-cycle	P3	TBD	TBD	TBD

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
SC-12	SC-12	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: encryption key generation, distribution, storage, access, and destruction is controlled by the agency.	Existing	P2	TBD	TBD	TBD
SC-13	SC-13	CRYPTOGRAPHIC PROTECTION	a. Determine the use of encryption for CJI in-transit when outside a physically secure location; and	Existing	P2	TBD	TBD	TBD
		"	b. Implement the following types of cryptography required for each specified cryptographic use: cryptographic modules which are Federal Information Processing Standard (FIPS) 140-3 certified, or FIPS validated algorithm for symmetric key encryption and decryption (FIPS 197 [AES]), with a symmetric cipher key of at least 128-bit strength for CJI in-transit.	Existing	P2	TBD	TBD	TBD
		"	NOTE: Subsequent versions of approved cryptographic modules that are under current review for FIPS 140-3 compliancy can be used in the interim until certification is complete. FIPS 140-2 certificates will not be acceptable after September 21, 2026.	Existing	P2	TBD	TBD	TBD
SC-15	SC-15	COLLABORATIVE COMPUTING DEVICES AND APPLICATIONS	a. Prohibit remote activation of collaborative computing devices and applications; and	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Provide an explicit indication of use to users physically present at the devices.	Zero-cycle	P2	TBD	TBD	TBD
SC-17	SC-17	PUBLIC KEY INFRASTRUCTURE CERTIFICATES	a. Issue public key certificates under an agency-level certificate authority or obtain public key certificates from an approved service provider; and	Existing	P2	Both	Service Provider	Service Provider
		"	b. Include only approved trust anchors in trust stores or certificate stores managed by the organization.	Existing	P2	Both	Service Provider	Service Provider
SC-18	SC-18	MOBILE CODE	a. Define acceptable and unacceptable mobile code and mobile code technologies; and	Zero-cycle	P3	TBD	TBD	TBD
		"	b. Authorize, monitor, and control the use of mobile code within the system.	Zero-cycle	P3	TBD	TBD	TBD
SC-20	SC-20	SECURE NAME/ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)	a. Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.	Zero-cycle	P2	TBD	TBD	TBD
SC-21	SC-21	SECURE NAME/ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)	Request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.	Zero-cycle	P2	TBD	TBD	TBD
SC-22	SC-22	ARCHITECTURE AND PROVISIONING FOR NAME/ADDRESS RESOLUTION SERVICE	Ensure the systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal and external role separation.	Zero-cycle	P2	TBD	TBD	TBD
SC-23	SC-23	SESSION AUTHENTICITY	Protect the authenticity of communications sessions.	Zero-cycle	P2	TBD	TBD	TBD

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
SC-28	SC-28	PROTECTION OF INFORMATION AT REST	Protect the confidentiality and integrity of the following information at rest: CJI when outside physically secure locations using cryptographic modules which are certified FIPS 140-3 with a symmetric cipher key of at least 128-bit strength, or FIPS 197 with a symmetric cipher key of at least 256-bit strength.	Existing	P2	Both	Service Provider	Service Provider
		"	Metadata derived from unencrypted CJI shall be protected in the same manner as CJI and shall not be used for any advertising or other commercial purposes by any cloud service provider or other associated entity.	Existing	P2	Both	Service Provider	Service Provider
		"	The storage of CJI, regardless of encryption status, shall only be permitted in cloud environments (e.g., government or third-party/commercial datacenters, etc.) which reside within the physical boundaries of APB-member country (i.e., United States, U.S. territories, Indian Tribes, and Canada) and are under legal authority of an APB-member agency (i.e., United States–federal/state/territory, Indian Tribe, or the Royal Canadian Mounted Police).	Existing	P2	Both	Service Provider	Service Provider
		"	Note: This restriction does not apply to exchanges of CJI with foreign government agencies under international exchange agreements (e.g., the Preventing and Combating Serious Crime agreements, fugitive extracts, and exchanges made for humanitarian and criminal investigatory purposes in particular circumstances).	Existing	P2	Both	Service Provider	Service Provider
SC-28 (1)	SC-28 (1)	PROTECTION OF INFORMATION AT REST CRYPTOGRAPHIC PROTECTION	Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on information systems and digital media outside physically secure locations: CJI.	Existing	P2	Both	Service Provider	Service Provider
SC-39	SC-39	PROCESS ISOLATION	Maintain a separate execution domain for each executing system process.	Existing	P2	Both	Service Provider	Service Provider

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy: System and Information Integrity (SI)								
5.15: SI-1	SI-1	POLICY AND PROCEDURES	a. Develop, document, and disseminate to all organizational personnel with system and information integrity responsibilities and information system owners:	Zero-cycle	P2	Agency	Agency	Agency
		"	1. Agency-level system and information integrity policy that:	Zero-cycle	P2	Agency	Agency	Agency
		"	(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Zero-cycle	P2	Agency	Agency	Agency
		"	(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and	Zero-cycle	P2	Agency	Agency	Agency
		"	2. Procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls;	Zero-cycle	P2	Agency	Agency	Agency
		"	b. Designate organizational personnel with system and information integrity responsibilities to manage the development, documentation, and dissemination of the system and information integrity policy and procedures; and	Zero-cycle	P2	Agency	Agency	Agency
		"	c. Review and update the current system and information integrity:	Zero-cycle	P2	Agency	Agency	Agency
		"	1. Policy annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI; and	Zero-cycle	P2	Agency	Agency	Agency
		"	2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.	Zero-cycle	P2	Agency	Agency	Agency
5.15: SI-2	SI-2	FLAW REMEDIATION	a. Identify, report, and correct system flaws;	Existing	P1	Both	Service Provider	Service Provider
		"	b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;	10/1/2024	P1	Both	Service Provider	Service Provider
		"	c. Install security-relevant software and firmware updates within the number of days listed after the release of the updates;	Existing	P1	Both	Service Provider	Service Provider
		"	• Critical – 15 days	10/1/2024	P1	Both	Service Provider	Service Provider
		"	• High – 30 days	10/1/2024	P1	Both	Service Provider	Service Provider
		"	• Medium – 60 days	10/1/2024	P1	Both	Service Provider	Service Provider
		"	• Low – 90 days; and	10/1/2024	P1	Both	Service Provider	Service Provider
		"	d. Incorporate flaw remediation into the organizational configuration management process.	10/1/2024	P1	Both	Service Provider	Service Provider
5.15: SI-2 (2)	SI-2 (2)	(2) FLAW REMEDIATION AUTOMATED FLAW REMEDIATION STATUS	Determine if system components have applicable security-relevant software and firmware updates installed using vulnerability scanning tools as least quarterly or following any security incidents involving CJI or systems used to process, store, or transmit CJI.	10/1/2024	P1	Both	Service Provider	Service Provider
5.15: SI-3	SI-3	MALICIOUS CODE PROTECTION	a. Implement signature-based malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;	10/1/2024	P1	Both	Service Provider	Service Provider
		"	b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;	Existing	P1	Both	Service Provider	Service Provider
		"	c. Configure malicious code protection mechanisms to:	Existing	P1			
		"	1. Perform periodic scans of the system at least daily and real-time scans of files from external sources at network entry and exit points and on all servers and endpoint devices as the files are downloaded, opened, or executed in accordance with organizational policy; and	Existing	P1	Both	Service Provider	Service Provider

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
5.15: SI-3	SI-3	MALICIOUS CODE PROTECTION (continued)	2. Block or quarantine malicious code, take mitigating action(s), and when necessary, implement incident response procedures; and send alert to system/network administrators and/or organizational personnel with information security responsibilities in response to malicious code detection; and	10/1/2024	P1	Both	Service Provider	Service Provider
		"	d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.	10/1/2024	P1	Both	Service Provider	Service Provider
5.15: SI-4	SI-4	SYSTEM MONITORING	a. Monitor the system to detect:	10/1/2024	P1	Both	Service Provider	Service Provider
		"	1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives:	10/1/2024	P1	Both	Service Provider	Service Provider
		"	a. Intrusion detection and prevention	10/1/2024	P1	Both	Service Provider	Service Provider
		"	b. Malicious code protection	10/1/2024	P1	Both	Service Provider	Service Provider
		"	c. Vulnerability scanning	10/1/2024	P1	Both	Service Provider	Service Provider
		"	d. Audit record monitoring	10/1/2024	P1	Both	Service Provider	Service Provider
		"	e. Network monitoring	10/1/2024	P1	Both	Service Provider	Service Provider
		"	f. Firewall monitoring;	10/1/2024	P1	Both	Service Provider	Service Provider
		"	2. Unauthorized local, network, and remote connections;	10/1/2024	P1	Both	Service Provider	Service Provider
		"	b. Identify unauthorized use of the system through the following techniques and methods: event logging (ref. 5.4 Audit and Accountability);	10/1/2024	P1	Both	Service Provider	Service Provider
		"	c. Invoke internal monitoring capabilities or deploy monitoring devices:	10/1/2024	P1	Both	Service Provider	Service Provider
		"	1. Strategically within the system to collect organization-determined essential information; and	10/1/2024	P1	Both	Service Provider	Service Provider
		"	2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;	10/1/2024	P1	Both	Service Provider	Service Provider
		"	d. Analyze detected events and anomalies;	10/1/2024	P1	Both	Service Provider	Service Provider
		"	e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;	10/1/2024	P1	Both	Service Provider	Service Provider
		"	f. Obtain legal opinion regarding system monitoring activities; and	10/1/2024	P1	Both	Service Provider	Service Provider
		"	g. Provide intrusion detection and prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring, and firewall monitoring software logs to organizational personnel with information security responsibilities weekly.	10/1/2024	P1	Both	Service Provider	Service Provider
5.15: SI-4 (2)	SI-4 (2)	(2) SYSTEM MONITORING AUTOMATED TOOLS AND MECHANISMS FOR REAL-TIME ANALYSIS	Employ automated tools and mechanisms to support near-real-time analysis of events.	Existing	P1	Both	Service Provider	Service Provider

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
5.15: SI-4 (4)	SI-4 (4)	(4) SYSTEM MONITORING INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC	a. Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic;	Existing	P1	Both	Service Provider	Service Provider
		"	b. Monitor inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions such as: the presence of malicious code or unauthorized use of legitimate code or credentials within organizational systems or propagating among system components, signaling to external systems, and the unauthorized exporting of information.	Existing	P1	Both	Service Provider	Service Provider
5.15: SI-4 (5)	SI-4 (5)	(5) SYSTEM MONITORING SYSTEM-GENERATED ALERTS	Alert organizational personnel with system monitoring responsibilities when the following system-generated indications of compromise or potential compromise occur: inappropriate or unusual activities with security or privacy implications.	Existing	P1	Both	Service Provider	Service Provider
5.12: SI-5	SI-5	SECURITY ALERTS, ADVISORIES, AND DIRECTIVES	a. Receive system security alerts, advisories, and directives from external source(s) (e.g., CISA, Multi-State Information Sharing & Analysis Center [MS-ISAC], U.S. Computer Emergency Readiness Team [USCERT], hardware/software providers, federal/state advisories, etc.) on an ongoing basis;	Existing	P2	Both	Service Provider	Service Provider
		"	b. Generate internal security alerts, advisories, and directives as deemed necessary;	Existing	P2	Both	Service Provider	Service Provider
		"	c. Issue security alerts, advisories, and directives to: organizational personnel implementing, operating, maintaining, and using the system; and	Existing	P2	Both	Service Provider	Service Provider
		"	d. Implement security directives in accordance with established time frames, or notify the issuing organization of the degree of noncompliance.	Existing	P2	Both	Service Provider	Service Provider
5.15: SI-7	SI-7	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY	a. Employ integrity verification tools to detect unauthorized changes to software, firmware, and information systems that contain or process CJI; and	10/1/2024	P1	Both	Service Provider	Service Provider
		"	b. Take the following actions when unauthorized changes to the software, firmware, and information are detected: notify organizational personnel responsible for software, firmware, and/or information integrity and implement incident response procedures as appropriate.	10/1/2024	P1	Both	Service Provider	Service Provider
5.15: SI-7 (1)	SI-7 (1)	(1) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY INTEGRITY CHECKS	Perform an integrity check of software, firmware, and information systems that contain or process CJI at agency-defined transitional states or security relevant events at least weekly or in an automated fashion.	10/1/2024	P1	Both	Service Provider	Service Provider
5.15: SI-7 (7)	SI-7 (7)	(7) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY INTEGRATION OF DETECTION AND RESPONSE	Incorporate the detection of the following unauthorized changes into the organizational incident response capability: unauthorized changes to established configuration setting or the unauthorized elevation of system privileges.	10/1/2024	P1	Both	Service Provider	Service Provider
5.15: SI-8	SI-8	SPAM PROTECTION	a. Employ spam protection mechanisms at system entry points to detect and act on unsolicited messages; and	Existing	P3	Both	Service Provider	Service Provider
		"	b. Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.	Existing	P3	Both	Service Provider	Service Provider
5.15: SI-8 (2)	SI-8 (2)	(2) SPAM PROTECTION AUTOMATIC UPDATES	Automatically update spam protection mechanisms at least daily.	Zero-cycle	P3	Both	Service Provider	Service Provider
5.15: SI-10	SI-10	INFORMATION INPUT VALIDATION	Check the validity of the following information inputs: all inputs to web/application servers, database servers, and any system or application input that might receive or process CJI.	10/1/2024	P1	Both	Service Provider	Service Provider
5.15: SI-11	SI-11	ERROR HANDLING	a. Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited; and	Zero-cycle	P3	Both	Service Provider	Service Provider
		"	b. Reveal error messages only to organizational personnel with information security responsibilities.	Zero-cycle	P3	Both	Service Provider	Service Provider

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
5.15: SI-12	SI-12	INFORMATION MANAGEMENT AND RETENTION	Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines and operational requirements.	Existing	P3	Both	Service Provider	Service Provider
5.15: SI-12 (1)	SI-12 (1)	(1) INFORMATION MANAGEMENT AND RETENTION LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS	Limit personally identifiable information being processed in the information life cycle to the minimum PII necessary to achieve the purpose for which it is collected (see Section 4.3).	Existing	P3	Both	Service Provider	Service Provider
5.15: SI-12 (2)	SI-12 (2)	(2) INFORMATION MANAGEMENT AND RETENTION MINIMIZE PERSONALLY IDENTIFIABLE INFORMATION IN TESTING, TRAINING, AND RESEARCH	Use the following techniques to minimize the use of personally identifiable information for research, testing, or training: data obfuscation, randomization, anonymization, or use of synthetic data.	Zero-cycle	P3	Both	Service Provider	Service Provider
5.15: SI-12 (3)	SI-12 (3)	(3) INFORMATION MANAGEMENT AND RETENTION INFORMATION DISPOSAL	Use the following techniques to dispose of, destroy, or erase information following the retention period: as defined in MP-6.	Existing	P3	Both	Service Provider	Service Provider
5.15: SI-16	SI-16	MEMORY PROTECTION	Implement the following controls to protect the system memory from unauthorized code execution: data execution prevention and address space layout randomization.	Zero-cycle	P2	Both	Service Provider	Service Provider

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy: Supply Chain Risk Management (SR)								
	SR-1	POLICY AND PROCEDURES	a. Develop, document, and disseminate to organizational personnel with supply chain risk management responsibilities:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. Agency-level supply chain risk management policy that:	Zero-cycle	P2	TBD	TBD	TBD
		"	a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and	Zero-cycle	P2	TBD	TBD	TBD
		"	2. Procedures to facilitate the implementation of the supply chain risk management policy and the associated supply chain risk management controls;	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Designate an organizational personnel with security responsibilities to manage the development, documentation, and dissemination of the supply chain risk management policy and procedures; and	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Review and update the current supply chain risk management:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. Policy annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI; and	Zero-cycle	P2	TBD	TBD	TBD
		"	2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.	Zero-cycle	P2	TBD	TBD	TBD
	SR-2	SUPPLY CHAIN RISK MANAGEMENT PLAN	a. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the following systems, system components or system services: systems used to process, store, or transmit CJI;	Zero-cycle	P3	TBD	TBD	TBD
		"	b. Review and update the supply chain risk management plan annually or as required, to address threat, organizational or environmental changes; and	Zero-cycle	P3	TBD	TBD	TBD
		"	c. Protect the supply chain risk management plan from unauthorized disclosure and modification.	Zero-cycle	P3	TBD	TBD	TBD
	SR-2(1)	(1) SUPPLY CHAIN RISK MANAGEMENT PLAN ESTABLISH SCRM TEAM	Establish a supply chain risk management team consisting of individuals with security responsibilities and supply chain risk management responsibilities to lead and support the following SCRM activities: information technology, contracting, information security, privacy, mission or business, legal, supply chain and logistics, acquisition, business continuity, and other relevant functions.	Zero-cycle	P3	TBD	TBD	TBD
	SR-5	ACQUISITION STRATEGIES, TOOLS, AND METHODS	Employ the following acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks: use preferred suppliers who can provide attestation or demonstration of compliance with state or federal standards.	Zero-cycle	P2	TBD	TBD	TBD
	SR-8	NOTIFICATION AGREEMENTS	Establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the notification of supply chain compromises to systems used to access, process, store, or transmit CJI.	Zero-cycle	P3	TBD	TBD	TBD
	SR-10	INSPECTION OF SYSTEMS OR COMPONENTS	Inspect the following systems or system components upon initial procurement and periodically as needed to detect tampering: systems used to access, process, store, or transmit CJI.	Zero-cycle	P3	TBD	TBD	TBD
	SR-12	COMPONENT DISPOSAL	Dispose of CJI using the techniques and methods as described in Media Protection (MP).	Zero-cycle	P3	TBD	TBD	TBD

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy Section 5-20: Mobile Devices								
5.13	5.20	Mobile Devices	The agency shall :	Existing	Existing			
		"	(i) establish usage restrictions and implementation guidance for mobile devices;	Existing	Existing	Agency	Agency	Agency
		"	(ii) authorize, monitor, control wireless access to the information system.	Existing	Existing	Agency	Agency	Agency
5.13.1.1	5.20.1.1	802.11 Wireless Protocols	Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) cryptographic algorithms, used by all pre-80.11i protocols, do not meet the requirements for FIPS 140-2 and shall not be used.	Existing	Existing	Agency	Agency	Agency
		"	Agencies shall implement the following controls for all agency-managed wireless access points with access to an agency's network that processes unencrypted CJI:	Existing	Existing	Agency	Agency	Agency
		"	1. Perform validation testing to ensure rogue APs (Access Points) do not exist in the 802.11 Wireless Local Area Network (WLAN) and to fully understand the wireless network security posture.	Existing	Existing	Agency	Agency	Agency
		"	2. Maintain a complete inventory of all Access Points (APs) and 802.11 wireless devices.	Existing	Existing	Agency	Agency	Agency
		"	3. Place APs in secured areas to prevent unauthorized physical access and user manipulation.	Existing	Existing	Agency	Agency	Agency
		"	4. Test AP range boundaries to determine the precise extent of the wireless coverage and design the AP wireless coverage to limit the coverage area to only what is needed for operational purposes.	Existing	Existing	Agency	Agency	Agency
		"	5. Enable user authentication and encryption mechanisms for the management interface of the AP.	Existing	Existing	Agency	Agency	Agency
		"	6. Ensure that all APs have strong administrative passwords and ensure that all passwords are changed in accordance with Identification and Authentication (IA).	Existing	Existing	Agency	Agency	Agency
		"	7. Ensure the reset function on APs is used only when needed and is only invoked by authorized personnel. Restore the APs to the latest security settings, when the reset functions are used, to ensure the factory default settings are not utilized.	Existing	Existing	Agency	Agency	Agency
		"	8. Change the default service set identifier (SSID) in the APs.	Existing	Existing	Agency	Agency	Agency
		"	Disable the broadcast SSID feature so that the client SSID must match that of the AP.	Existing	Existing	Agency	Agency	Agency
		"	Validate that the SSID character string does not contain any agency identifiable information (division, department, street, etc.) or services.	Existing	Existing	Agency	Agency	Agency
		"	9. Enable all security features of the wireless product, including the cryptographic authentication, firewall, and other privacy features.	Existing	Existing	Agency	Agency	Agency
		"	10. Ensure that encryption key sizes are at least 128-bits and...	Existing	Existing	Agency	Agency	Agency
		"	...and the default shared keys are replaced by unique keys.	Existing	Existing	Agency	Agency	Agency
		"	11. Ensure that the ad hoc mode has been disabled.	Existing	Existing	Agency	Agency	Agency
		"	12. Disable all nonessential management protocols on the APs. Disable non-FIPS compliant secure access to the managment interface.	Existing	Existing	Agency	Agency	Agency
		"	13. Ensure all management access and authentication occurs via FIPS compliant secure protocols (e.g. SFTP, HTTPS, SNMP over TLS, etc.). Disable non-FIPS compliant secure access to the managment interface.	Existing	Existing	Agency	Agency	Agency
		"	14. Enable logging (if supported) and...	Existing	Existing	Agency	Agency	Agency
		"	...and review the logs on a recurring basis per local policy.	Existing	Existing	Agency	Agency	Agency
		"	At a minimum logs shall be reviewed monthly.	Existing	Existing	Agency	Agency	Agency

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
5.13.1.1	5.20.1.1	802.11 Wireless Protocols (continued)	15. Insulate, virtually (e.g. virtual local area network (VLAN) and ACLs) or physically (e.g. firewalls), the wireless network from the operational wired infrastructure.	Existing	Existing	Agency	Agency	Agency
		"	16. When disposing of access points that will no longer be used by the agency, clear access point configuration to prevent disclosure of network configuration, keys, passwords, etc.	Existing	Existing	Agency	Agency	Agency
5.13.1.2.1	5.20.1.2.1	Cellular Service Abroad	When devices are authorized to access CJI outside the U.S., agencies shall perform an inspection to ensure that all controls are in place and functioning properly in accordance with the agency's policies prior to and after deployment outside of the U.S.	Existing	Existing	Agency	Agency	Agency
5.13.1.3	5.20.1.3	Bluetooth	Organizational security policy shall be used to dictate the use of Bluetooth and its associated devices based on the agency's operational and business processes.	Existing	Existing	Agency	Agency	Agency
5.13.1.4	5.20.1.4	Mobile Hotspots	When an agency allows mobile devices that are approved to access or store CJI to function as a Wi-Fi hotspot connecting to the Internet, they shall be configured:	Existing	Existing			
		"	1. Enable encryption on the hotspot	Existing	Existing	Agency	Agency	Agency
		"	2. Change the hotspot's default SSID	Existing	Existing	Agency	Agency	Agency
		"	a. Ensure the hotspot SSID does not identify the device make/model or agency ownership	Existing	Existing	Agency	Agency	Agency
		"	3. Create a wireless network password (Pre-shared key)	Existing	Existing	Agency	Agency	Agency
		"	4. Enable the hotspot's port filtering/blocking features if present	Existing	Existing	Agency	Agency	Agency
		"	5. Only allow connections from agency controlled devices	Existing	Existing	Agency	Agency	Agency
5.13.2	5.20.2	"	OR 1. Have a MDM solution to provide the same security as identified in 1 - 5 above.	Existing	Existing	Agency	Agency	Agency
		Mobile Device Management (MDM)	Devices that have had any unauthorized changes made to them (including but not limited to being rooted or jailbroken) shall not be used to process, store, or transmit CJI at any time.	Existing	Existing	Agency	Agency	Agency
		"	User agencies shall implement the following controls when directly accessing CJI from devices running limited feature operating system:	Existing	Existing			
		"	1. Ensure that CJI is only transferred between CJI authorized applications and storage areas of the device.	Existing	Existing	Agency	Agency	Agency
		"	2. MDM with centralized administration configured and implemented to perform at least the following controls:	Existing	Existing	Agency	Agency	Agency
		"	a. Remote locking of the device	Existing	Existing	Agency	Agency	Agency
		"	b. Remote wiping of the device	Existing	Existing	Agency	Agency	Agency
		"	c. Setting and locking device configuration	Existing	Existing	Agency	Agency	Agency
		"	d. Detection of "rooted" and "jailbroken" devices	Existing	Existing	Agency	Agency	Agency
		"	e. Enforcement of folder or disk level encryption	Existing	Existing	Agency	Agency	Agency
		"	f. Application of mandatory policy settings on the device	Existing	Existing	Agency	Agency	Agency
		"	g. Detection of unauthorized configurations	Existing	Existing	Agency	Agency	Agency
		"	h. Detection of unauthorized software or applications	Existing	Existing	Agency	Agency	Agency
		"	i. Ability to determine location of agency controlled devices	Existing	Existing	Agency	Agency	Agency
		"	j. Prevention of unpatched devices from accessing CJI or CJI systems	Existing	Existing	Agency	Agency	Agency
		"	k. Automatic device wiping after a specified number of failed access attempts	Existing	Existing	Agency	Agency	Agency

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
5.13.3	5.20.3	Wireless Device Risk Mitigations	Organizations shall , as a minimum, ensure that wireless devices:	Existing	Existing			
		"	1. Apply available critical patches and upgrades to the operating system as soon as they become available for the device and after necessary testing as described in System and Information Integrity (SI).	Existing	Existing	Agency	Agency	Agency
		"	2. Are configured for local device authentication (see Section 5.20.8.1).	Existing	Existing	Agency	Agency	Agency
		"	3. Use advanced authentication or CSO approved compensating controls as per Section 5.20.7.2.1.	Existing	Existing	Agency	Agency	Agency
		"	4. Encrypt all CJI resident on the device.	Existing	Existing	Agency	Agency	Agency
		"	5. Erase cached information, to include authenticators (see Identification and Authentication (IA)) in applications, when session is terminated.	Existing	Existing	Agency	Agency	Agency
		"	6. Employ personal firewalls on full-featured operating system devices or run a Mobile Device Management (MDM) system that facilitates the ability to provide firewall services from the agency level.	Existing	Existing	Agency	Agency	Agency
		"	7. Employ malicious code protection on full-featured operating system devices or run a MDM system that facilitates the ability to provide anti-malware services from the agency level.	Existing	Existing	Agency	Agency	Agency
5.13.4.1	5.20.4.1	Patching/Updates	Agencies shall monitor mobile devices to ensure their patch and update state is current.	Existing	Existing	Agency	Agency	Agency
5.13.4.2	5.20.4.2	Malicious Code Protection	Agencies that allow smartphones and tablets to access CJI shall have a process to approve the use of specific software or applications on the devices.	Existing	Existing	Agency	Agency	Agency
5.13.4.3	5.20.4.3	Personal Firewall	A personal firewall shall be employed on all devices that have a full-feature operating system (i.e. laptops or tablets with Windows or Linux/Unix operating systems).	Existing	Existing	Agency	Agency	Agency
		"	At a minimum, the personal firewall shall perform the following activities:	Existing	Existing			
		"	1. Manage program access to the Internet.	Existing	Existing	Agency	Agency	Agency
		"	2. Block unsolicited requests to connect to the PC.	Existing	Existing	Agency	Agency	Agency
		"	3. Filter Incoming traffic by IP address or protocol.	Existing	Existing	Agency	Agency	Agency
		"	4. Filter Incoming traffic by destination ports.	Existing	Existing	Agency	Agency	Agency
5.13.5	5.20.5	"	5. Maintain an IP traffic log.	Existing	Existing	Agency	Agency	Agency
		Incident Response	In addition to the requirements in Section 5.3 Incident Response, agencies shall develop additional or enhanced incident reporting and handling procedures to address mobile device operating scenarios.	Existing	Existing	Agency	Agency	Agency
		"	Special reporting procedures for mobile devices shall apply in any of the following situations:	Existing	Existing			
		"	1. Loss of device control. For example:	Existing	Existing	Agency	Agency	Agency
		"	a. Device known to be locked, minimal duration of loss	Existing	Existing	Agency	Agency	Agency
		"	b. Device lock state unknown, minimal duration of loss	Existing	Existing	Agency	Agency	Agency
		"	c. Device lock state unknown, extended duration of loss	Existing	Existing	Agency	Agency	Agency
		"	d. Device known to be unlocked, more than momentary duration of loss	Existing	Existing	Agency	Agency	Agency
5.13.6	5.20.6	Access Control	2. Total loss of device	Existing	Existing	Agency	Agency	Agency
			3. Device compromise	Existing	Existing	Agency	Agency	Agency
			4. Device loss or compromise outside the United States	Existing	Existing	Agency	Agency	Agency
			Access control (see Access Control (AC)) shall be accomplished by the application that accesses CJI.	Existing	Existing	Agency	Agency	Agency

Ver 5.9.5 Location and New Requirement	Ver 6.0 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
5.13.7.1	5.20.7.1	Local Device Authentication	When mobile devices are authorized for use in accessing CJI, local device authentication shall be used to unlock the device for use.	Existing	Existing	Agency	Agency	Agency
		"	The authenticator used shall meet the requirements in Identification and Authentication (IA).	Existing	Existing	Agency	Agency	Agency
5.13.7.2	5.20.7.2	Advanced Authentication	When accessing CJI from an authorized mobile device, advanced authentication shall be used by the authorized user unless the access to CJI is indirect as described in Identification and Authentication (IA). If access is indirect, then AA is	Existing	Existing	Agency	Agency	Agency
5.13.7.2.1	5.20.7.2.1	Compensating Controls	Before CSOs consider approval of compensating controls, Mobile Device Management (MDM) shall be implemented per Section 5.20.2.	Existing	Existing	Agency	Agency	Agency
		"	The compensating controls shall :	Existing	Existing			
		"	1. Meet the intent of the CJIS Security Policy AA requirement	Existing	Existing	Agency	Agency	Agency
		"	2. Provide a similar level of protection or security as the original AA requirement	Existing	Existing	Agency	Agency	Agency
		"	3. Not rely upon the existing requirements for AA as compensating controls	Existing	Existing	Agency	Agency	Agency
		"	4. Expire upon the CSO approved date or when a compliant AA solution is implemented.	Existing	Existing	Agency	Agency	Agency
		"	The following minimum controls shall be implemented as a part of the CSO approved compensating controls:	Existing	Existing			
		"	Possession and registration of an agency-issued smartphone or tablet as an indication it is the authorized user	Existing	Existing	Agency	Agency	Agency
		"	Use of device certificates as per Section 5.20.7.3 Device Certificates	Existing	Existing	Agency	Agency	Agency
		"	Implemented CJIS Security Policy compliant standard authenticator protection on the secure location where CJI is stored	Existing	Existing	Agency	Agency	Agency
5.13.7.3	5.20.7.3	Device Certificates	When certificates or cryptographic keys used to authenticate a mobile device are used in lieu of compensating controls for advanced authentication, they shall be:	Existing	Existing			
		"	1. Protected against being extracted from the device	Existing	Existing	Agency	Agency	Agency
		"	2. Configured for remote wipe on demand or self-deletion based on a number of unsuccessful login or access attempts	Existing	Existing	Agency	Agency	Agency
		"	3. Configured to use a secure authenticator (i.e. password, PIN) to unlock the key for use	Existing	Existing	Agency	Agency	Agency



RESPONSIBILITIES OF THE AUTHORIZED RECIPIENT POINT OF CONTACT

Noncriminal Justice Purposes

Responsibility	Explanation
Authorized Personnel List	Submits and maintains a current authorized personnel list to the Department of Public Safety civil auditor.
Audits	Cooperates with State or Federal officials during the audit process. Maintains all required audit documentation and serves as the agency representative for audits. Completes all documentation required during the audit and submits any required corrective action documentation in a timely manner.
Changes	Notify civil auditor within 10 business days of any changes in agency name, address, phone number, contact person or status of the agency, by submission of a change form.
Primary Liaison	Person through which all communication regarding audits, training and security is conducted. First contact person for the Department of Public Safety.
Training	Ensures authorized personnel receive required training and receive the criminal history records information misuse acknowledgement understanding the use, dissemination, storage, destruction and penalties for misuse.
Compliance in Privacy and Security	Maintains copies of authorized personnel training certificates on file. Maintains Dissemination logs (if applicable). Ensures agency has policies /procedures related to access, use, handling, dissemination, and destruction of State and National fingerprint-based criminal history records.



Nevada Department of
Public Safety
Dedication Pride Service

Records, Communications and Compliance Division
333 West Nye Lane, Suite 100
Telephone (775) 684-6262
ap@dps.state.nv.us
Carson City, Nevada 89706
Fax (775) 687-3232
www.rccd.nv.gov

CIVIL APPLICANT ACCOUNT UPDATE FORM

(one account per form) **ALL information is required unless noted "if applicable". Incomplete forms may result in a processing delay.**

For use by DPS RCCD Staff Only

☐ No Changes
FISCAL

☐ No Changes
FSU

Processed By: _____

Date: _____

Website: _____

RCCD Account
Number: _____

Company
Name: _____

Federal Tax ID # *if "New", please provide a copy of the Federal Tax ID letter

☐ Current _____

**Statutory
Authority**
(If Applicable)

☐ Add _____

☐ New* _____

☐ Delete _____

Address Change – applies to (CHECK ALL THAT APPLY):

Physical Address _____

City – State – Zip _____

Billing Address _____

City – State – Zip _____

Response Address _____

City – State – Zip _____

Contact Information - applies to (CHECK ALL THAT APPLY): ☐ Billing ☐ Response ☐ Both ☐ Add ☐ Delete

Name and Title (printed) _____

Telephone Number _____

E-mail Address _____

Fax Number _____

Contact Information - applies to (CHECK ALL THAT APPLY): ☐ Billing ☐ Response ☐ Both ☐ Add ☐ Delete

Name and Title (printed) _____

Telephone Number _____

E-mail Address _____

Fax Number _____

Contact Information - applies to (CHECK ALL THAT APPLY): ☐ Billing ☐ Response ☐ Both ☐ Add ☐ Delete

Name and Title (printed) _____

Telephone Number _____

E-mail Address _____

Fax Number _____

Terms: Statements will be mailed each month. In order to maintain a current account, the balance in full must be paid within 10 days of receipt. If a credit limit is granted for this application, the account may be suspended if the credit limit is exceeded or if the account is not current. If an account is suspended, services will not be provided until the account terms are satisfied. Any change to organization information including address must be reported within 10 business days.

****Any payment on account
returned for Non-Sufficient
Funds will be assessed a
\$25.00 fee.****

I, the undersigned, have the authority to make the changes outlined herein on behalf of the Company/Organization listed above. I agree to the terms listed above and I understand that any credit limit associated with this account is at the discretion of the Department of Public Safety, Records, Communications and Compliance Division.

Authorized Company Representative Signature _____

Date _____

Authorized Company Representative Name-PRINTED _____

Title _____



Nevada Department of **Public Safety** Fingerprint Background Waiver

As an applicant who is the subject of a national fingerprint-based criminal history record check for a noncriminal justice purpose (such as an application for employment or a license, an immigration or naturalization matter, security clearance, or adoption), you have certain rights which are discussed below. All notices must be provided to you in writing. These obligations are pursuant to the Privacy Act of 1974, Title 5, United States Code (U.S.C.) Section 552a, and Title 28 Code of Federal Regulations (CFR), 50.12, among other authorities.

1. You must be notified by _____ (*name of requesting agency*) that your fingerprints will be used to check the criminal history records of the FBI and the State of Nevada.
2. **Authority:** The FBI's acquisition, preservation, and exchange of fingerprints and associated information is generally authorized under 28 U.S.C. 534. Depending on the nature of your application, supplemental authorities include Federal statutes, State statutes pursuant to Pub. L. 92-544, Presidential Executive Orders, and federal regulations. Providing your fingerprints and associated information is voluntary; however, failure to do so may affect completion or approval of your application.
3. **Principal Purpose:** Certain determinations, such as employment, licensing, and security clearances, may be predicated on fingerprint-based background checks. Your fingerprints and associated information/biometrics may be provided to the employing, investigating, or otherwise responsible agency, and/or the FBI for the purpose of comparing your fingerprints to other fingerprints in the FBI's Next Generation Identification (NGI) system or its successor systems (including civil, criminal, and latent fingerprint repositories) or other available records of the employing, investigating, or otherwise responsible agency. The FBI may retain your fingerprints and associated information/biometrics in NGI after the completion of this application and, while retained, your fingerprints may continue to be compared against other fingerprints submitted to or retained by NGI.
4. **Routine Uses:** During the processing of this application and for as long thereafter as your fingerprints and associated information/biometrics are retained in NGI, your information may be disclosed pursuant to your consent, and may be disclosed without your consent as permitted by the Privacy Act of 1974 and all applicable Routine Uses as may be published at any time in the Federal Register, including the Routine Uses for the NGI system and the FBI's Blanket Routine Uses. Routine uses include, but are not limited to, disclosures to: employing, governmental or authorized non-governmental agencies responsible for employment, contracting, licensing, security clearances, and other suitability determinations; local, state, tribal, or federal law enforcement agencies; criminal justice agencies; and agencies responsible for national security or public safety.
5. If you have a criminal history record, you should be afforded a reasonable amount of time to correct or complete the record (or decline to do so) before the officials deny you the employment, license, or other benefit based on information in the FBI criminal history record. The procedures for obtaining a change, correction, or update of your FBI criminal history record as set forth at, 28 CFR 16.34 provides for the proper procedure to do so.

Applicant:

Initial

Date

6. If agency policy permits, the officials may provide you with a copy of your FBI criminal history record for review and possible challenge. If agency policy does not permit it to provide you a copy of the record, you may obtain a copy of the record by submitting fingerprints and a fee to the FBI. Information regarding this process may be obtained at <https://www.fbi.gov/services/cjis/identity-history-summary-checks> and <https://www.edo.cjis.gov>.
7. If you decide to challenge the accuracy or completeness of your FBI criminal history record, you should send your challenge to the agency that contributed the questioned information to the FBI. Alternatively, you may send your challenge directly to the FBI by submitting a request via <https://www.edo.cjis.gov>. The FBI will then forward your challenge to the agency that contributed the questioned information and request the agency to verify or correct the challenged entry. Upon receipt of an official communication from that agency, the FBI will make any necessary changes/corrections to your record in accordance with the information supplied by that agency. (See 28 CFR 16.30 through 16.34.)
8. You have the right to expect that officials receiving the results of the fingerprint-based criminal history record check will use it only for authorized purposes and will not retain or disseminate it in violation of federal or state statute, regulation or executive order, or rule, procedure or standard established by the National Crime Prevention and Privacy Compact Council.
9. I hereby authorize _____ (*name of requesting agency*), to submit a set of my fingerprints to the Nevada Department Public Safety, Records Bureau for the purpose of accessing and reviewing State of Nevada and FBI criminal history records that may pertain to me.
10. I hereby release from liability and promise to hold harmless under any and all causes of legal action, the State of Nevada, its officer(s), agent(s) and/or employee(s) who conducted my criminal history records search and provided information to the submitting agency for any statement(s), omission(s), or infringement(s) upon my current legal rights. I further release and promise to hold harmless and covenant not to sue any persons, firms, institutions or agencies providing such information to the State of Nevada on the basis of their disclosures. I have signed this release voluntarily and of my own free will.

A reproduction of this authorization for release of information by photocopy, facsimile or similar process, shall for all purposes be as valid as the original.

In consideration for processing my application I, the undersigned, whose name and signature voluntarily appears below; do hereby and irrevocably agree to the above.

Applicant's Name:

PLEASE PRINT

Last Name

First Name

Middle

Applicant's Signature: _____

Date: _____

Agency Account #: _____

Agency Representative: _____

PLEASE PRINT

Last Name

First Name

Middle

Agency Representative Signature: _____

Date: _____

Joe Lombardo
Governor



Nevada Department of
Public Safety
Records, Communications and Compliance

George Togliatti
Director

**Record, Communications and
Compliance Division**
333 West Nye Lane, Suite 100
Carson City, Nevada 89706
Telephone (775) 684-6262 – Fax (775) 684-6265
www.rccd.nv.gov

Erica Souza-Llamas
Division Administrator

July 30, 2021

Notification for Civil Applicant Account Holders

The State of Nevada Department of Public Safety (DPS) Record, Communications and Compliance Division is the liaison between the State of Nevada and the Federal Bureau of Investigation (FBI) for fingerprint submissions as required by State or Federal Law for employment or licensing.

In order to reduce unnecessary handling, processing errors, billing issues and invalid dissemination of the Criminal History Record Information we are asking that each account holder create a Fingerprint Request Form to provide to their applicants. The implementation of the Fingerprint Request Form, as a “Best Business Practice”, will ensure that your applicant is presenting all of the required and authorized information to the fingerprinting site.

We have included a sample Fingerprint Request Form to assist you in developing a document specific to your agency or business entity. This form contains all of the information that is required for successfully processing fingerprints for State and FBI criminal history background checks. Additionally, the sample form includes a section for applicant information, authorized entity information (agency or business entity) and the fingerprint site information.

We really appreciate your cooperation and willingness to implement this “Best Business Practice”. The creation of the Fingerprint Request Form specific to your agency or business entity will help ensure that you are receiving responses and monthly billing for only your applicants.

Please feel free to contact us with any questions that you may have.

Fingerprint Support Unit
(775) 684-6262

Thank you!

0506RCCD-001(07/2021rev)

*Your Entity Name/Letterhead
Address/Contact information*

FINGERPRINT REQUEST FORM

Please provide this form to the fingerprint technician/official at the time the fingerprints are taken to ensure that all fields contain the required/authorized information needed for processing. ***Applicants without a Fingerprint Request Form or with an incomplete Fingerprint Request Form may be denied fingerprinting until all applicable information is received.***

Fingerprint technician, please ensure that you see photo ID for identity verification purposes prior to fingerprinting.

Applicant Information:

Name (Last, First, MI): _____

Address: _____

City, State and Zip: _____

Date of Birth: _____ Place of Birth: _____

SSN (if required): _____ Citizenship: _____

Sex: _____ Race: _____ Height: _____ Weight: _____ Eyes: _____ Hair: _____

Authorized Entity Information:

Account Number (MNU): _____ ORI: _____

Applicant Responsible for Fees: ☐ --OR-- Bill to Account Number (MNU) _____

Reason Fingerprinted (NRS or Public Law) _____

Submit Fingerprints Electronic LiveScan: Yes No

If NO, please print hard cards and return to applicant for manual submission.

****Signature of Authorization:**

(Signature of Employer or Authorized Entity requesting fingerprints)

Fingerprint Site Information:

Signature of Official Taking Prints: _____

TCN Number (used for tracking purposes): _____

SECONDARY DISSEMINATION LOG

[illegible]

- An applicant with a disqualifying out-of-state arrest applied for a teacher certificate and persuaded a student to provide the applicant her fingerprints. The fingerprints were submitted and the applicant was able to obtain a teaching certificate. The student subsequently was arrested and the fingerprints hit on her own fingerprints that were in the state rap back system. When the Department of Education received the rap back notification, they discovered that the mug shot did not match the teacher enrolled in rap back. An investigation revealed identity fraud and the case was turned over for criminal prosecution of both the teacher applicant and the student. In this instance rap back prevented a disqualified individual from having continued access to a vulnerable population.
2. The following scenario illustrates how an applicant attempted to circumvent the fingerprinting process in order to obtain a position of trust, but due to the vigilance of the fingerprinting vendor, the hiring agency was able to successfully prevent the individual from obtaining the position.
- An individual applied for a health care worker position. Due to the fact that she had a criminal history record, she requested her roommate be fingerprinted on her behalf. Unbeknownst to her, the roommate also had a record. However, the fingerprinting agency verified the applicant's identification and determined that the photo/biographic identification did not match the applicant's identity. The fingerprint vendor notified the Department of Health (DPH) that the applicant did not match the identification submitted. Subsequently, both the applicant and the individual that agreed to submit the false fingerprints were arrested and charged. Due to verification of the identification, the DPH was able to detect fingerprint fraud and prevent a convicted felon from obtaining a position of trust as a health care worker.

Federal Legislation and Other Documents Pertinent to this Guide:

34 U.S.C. § 40316 (formerly cited as 42 U.S.C. § 14616)

Public Law 109-13, also referred to as the REAL ID Act
(The Emergency Supplemental Appropriations Act for Defense,
the Global War on Terror, and Tsunami Relief Act, May 11, 2005)

HSPD-12 (Homeland Security Presidential Directive - 12)

Revised 2014 by the National Crime Prevention and Privacy Compact Council

Identity Verification Program Guide



The National Crime Prevention and Privacy Compact Council (Compact Council) is a 15-member body of local, state, and federal governmental officials which prescribes system rules and procedures for the effective and proper operation of the Interstate Identification Index (III) for noncriminal justice purposes.

In recent years, the demand for fingerprint-based background checks for noncriminal justice purposes has increased. Fingerprinting agencies and contractors alike have expressed concern that applicants with a criminal history record may have someone pose as the applicant for fingerprinting purposes. In response to these concerns, the Compact Council prepared this guide for voluntary use in the development of policy, procedures, and practices for applicant identity verification.

FACTORS TO CONSIDER

(For the purpose of this guide, “agency” will refer to any agency or contractor responsible for the capture and/or submission of fingerprints for noncriminal justice purposes.)

In the course of establishing an identity verification program, agencies may choose to consider the following factors:

- Clearly define and document policy, procedure, and practices. Document what is to be accomplished and how it is to be performed.
- Review current business policy, procedure, and practices regarding verification, training, legal obligations, and privacy implications that may be incorporated into a program.
- Develop an understanding of the use of various biometric-based systems.

PRELIMINARY CONSIDERATIONS

Coordination with the State Repository

Since the state repository manages the processing of fingerprint submissions to the FBI, it is suggested that appropriate coordination and liaison be established at that level as a preliminary step toward an identity verification program.

E. Implement the use of form(s), which may include the:

1. Date of fingerprinting
2. Reason for fingerprinting
3. Printed name, signature, and/or identification number of the employee taking the fingerprints
4. Name of employee’s supervisor
5. Supervisor’s signature
6. Address of agency to receive fingerprints
7. Name of agency and physical address where fingerprinting was performed
8. Type of fingerprint capture (rolled ink, flat ink, live scan, etc.)
9. Applicant’s consent for fingerprinting
10. Type of ID verified (Driver’s License #/State/Expiration Date)

For further information, please visit the Compact Council website at:

www.fbi.gov/services/cjis/compact-council

FINGERPRINT FRAUD SCENARIOS

1. The following scenarios illustrate how an applicant attempted and successfully circumvented the fingerprinting process in order to obtain a position of trust and the importance of verifying the individual’s identity, as well as maintaining the chain-of-custody:
 - An individual applied for, and successfully obtained, a position of trust as a teacher within a school district, after having another individual go to the sheriff’s office and provide his fingerprints. The prospective teacher also utilized his father’s name, which was the same as his. The fingerprints were subsequently submitted to the State Identification Bureau for a background check. Two years later, the falsified fingerprints were discovered when the teacher was arrested for criminal trespass and window peeping. It was also discovered the teacher had a prior arrest and conviction for simple assault and a sexual battery arrest which resulted in a misdemeanor assault conviction. As a result, the individual’s employment was terminated. Subsequently, the individual who had submitted the falsified fingerprints was also arrested for fraudulent activity.

- Check the applicant's signature in person with that on the identification form.
- Ensure that the identification form has not been altered in any manner.
- If available, verify that the machine readable data matches the data on the card when it is scanned.

When an agency has a reason to believe an applicant has presented fraudulent information, agency personnel should contact local law enforcement. No attempt should be made to detain or pursue the person.

CREATE CHAIN OF CUSTODY PROCEDURES

An agency may employ a process to protect the integrity of the applicant's fingerprints when they are forwarded to the state identification bureau and/or the FBI. The following information provides a guide to developing a chain of custody process:

- Establish provisions for the agency to manage both manually and electronically captured fingerprints.
- Establish an agency tracking system (applicant log) using the employee's name or some other method of identifying the individual capturing the fingerprints and verifying the applicant's identity.
- Establish procedures that document the type(s) of identification used by the applicant.
- When possible, electronic fingerprint submissions should be used, thus eliminating the return of the fingerprint card to the applicant. However, in those instances when the fingerprints must be returned to the applicant, the agency should establish procedures that use specially sealed envelopes, agency specific stamps, etc. when forwarding the applicant's manually captured fingerprints.

Fingerprinter Certification

Another preliminary consideration for states may be the enacting of a state statute establishing a certification process that qualifies the employees capturing the applicant's fingerprints. Additionally, if the statute were compliant with Public Law 92-544, a state and federal fingerprint-based background check could be performed on the individuals certified to take fingerprints.

POLICY, PROCEDURES, AND PRACTICES

In developing an identity verification program, the Compact Council suggests establishing written policy, procedures, and practices. The following guide may be helpful in the process.

- Determine Policy, Procedures, and Practices
- Create an Identification Validation Guide
- Create Chain of Custody Procedures

Determine Policy, Procedures and Practices

Policy, Procedures, and Practices may include:

- Training in the capture of fingerprints (rolled or flats, and hard copy or livescan).
- Certification of employees performing duties under the scope of the identity verification program, which may include recognizing and validating authorized identification forms, identification documents, and source documents for identity confirmation.
- Security considerations:
 - Train employees to recognize and properly utilize the security features of the various forms of identification presented. These features include biometric like photographs and machine-readable technology such as magnetic strips and 2D/3D barcodes.
 - Assign a unique identification number to each employee to be included with each fingerprint submission.

Create an Identification Validation Guide

Primary and Secondary Identification

Currently most agencies request some type of photo identification card as one method for verifying an individual's identity. The Compact Council suggests agencies accept only current, valid, and unexpired photo identification documents.

As a primary form of photo identification, the following documents may be presented by an applicant when being fingerprinted:

- State-issued driver's license*
- U.S. Passport or U.S. Passport Card
- Federal Government Personal Identity Verification Card (PIV)
- Uniformed Services Identification Card
- Department of Defense Common Access Card
- Foreign Passport with Appropriate Immigration Document(s)
- USCIS - Permanent Resident Card (I-551)
- USCIS - Employment Authorization Card (I-766)
- Federal, state, or local government agency ID card with photograph
- U.S. Coast Guard Merchant Mariner Card
- Canadian driver's license

* For those applicants without a driver's license, a state identification card may be presented if the state's identification card standards are the same as for the driver's license.

However, in the absence of a primary identification, applicants may provide at least 2 secondary identification documents including:

- State Government Issued Certificate of Birth
- U.S. Tribal or Bureau of Indian Affairs Identification Card
- Native American tribal document
- Social Security Card
- Court Order for Name Change/Gender Change/Adoption/Divorce

- Marriage Certificate (Government Certificate Issued)
- U.S. Government Issued Consular Report of Birth Abroad
- Draft record
- School ID with photograph
- Certificate of Citizenship (N-560)
- Replacement Certificate of Citizenship (N-561)
- Certificate of Naturalization (N-550)
- Replacement Certificate of Naturalization (N-570)

Secondary Identification Data Support Documents

When validating the authenticity of secondary identification documents and forms, the data and information may be supported by at least two of the following current documents:

- Utility Bill (Address)
- Jurisdictional Voter Registration Card
- Vehicle Registration Card/Title
- Paycheck Stub with Name/Address*
- Jurisdictional Public Assistance Card
- Spouse/Parent Affidavit

* Financial information may be redacted by the individual.

Additional Identification Data Support Methods

To further support the validation of the original identification documents, the agency may choose any or all of the following methods to validate the authenticity of the documents:

- Physically examine the applicant's photo on the identification form/card. Visually compare the photo with the applicant in person.
- Compare the physical descriptors of the applicant to the documentation provided by the applicant (i.e. height, weight, hair and eye color, age, etc.).
- Request the applicant to verbally provide date of birth, address, etc., and check this against the identification forms used.

NOTICE

The Storey County Sheriff's Office certify that the fingerprint cards in this envelope have been placed in this envelope to ensure security and chain of custody of the fingerprint cards.

Signed by: *[Signature]*

Date: *11/15/2010*

Applicant was verified by photo ID

P. O. Box 498 Virginia City, Nevada 89440
(775) 847-0959 or sheriff@storeycountynv.org

NOTICE

Based on the Federal Reg. 42USC1437D (Q) Fingerprints
Submitted for Housing Eligibility/Employment

_____) certify that the fingerprint cards in this
Fingerprinting Entity

envelope have been placed in this envelope to ensure security
and chain of custody of the fingerprint cards.

Signed by: _____

Date: _____

FingerprintCert.doc 05/18/2009 #33316

Technician: After placing the fingerprint cards in the attached envelope, please affix
this notice over the seal of the envelope.
Thank you.

CHAIN OF CUSTODY SAMPLE LABELS

Criminal History Record Information Misuse Acknowledgment

Understand the following:

1. **Criminal History Record Information (CHRI) must be used only for the purpose for which it was provided.**
2. **CHRI cannot be disseminated outside of the receiving department, related agencies, or other authorized entities.**
3. **CHRI must be maintained in a secured records environment.**
4. **CHRI, if destroyed, must be shredded or burned.**

NATIONAL CRIME PREVENTION AND PRIVACY COMPACT

NRS 179A.800 Enactment; text. The National Crime Prevention and Privacy Compact is hereby ratified, enacted into law and entered into with all jurisdictions legally joining in the Compact, in substantially the form set forth in this section:

Article IV. Authorized Record Disclosures

(1) To the extent authorized by section 552a of Title 5, United States Code (commonly known as the Privacy Act of 1974), the FBI shall provide on request criminal history records, excluding sealed record information, to state criminal history record repositories for noncriminal justice purposes allowed by federal statute, federal executive order, or a state statute which has been approved by the Attorney General and which authorizes national indexes checks.

(2) The FBI, to the extent authorized by section 552a of Title 5, United States Code (commonly known as the Privacy Act of 1974), and state criminal history record repositories shall provide criminal history records, excluding sealed record information, to criminal justice agencies and other governmental or nongovernmental agencies for noncriminal justice purposes allowed by federal statute, federal executive order, or a state statute that has been approved by the Attorney General, that explicitly authorizes national indexes checks.

(3) Any record obtained under this Compact may be used only for the official purposes for which the record was requested. Each Compact officer shall establish procedures, consistent with this Compact and with rules, procedures, and standards established by the Council under Article VI, which procedures shall protect the accuracy and privacy of the records and shall:

(a) Ensure that records obtained under this Compact are used only by authorized officials for authorized purposes;

(b) Require that subsequent record checks are requested to obtain current information whenever a new need arises; and

(c) Ensure that record entries that may not legally be used for a particular noncriminal justice purpose are deleted from the response and, if no information authorized for release remains, an appropriate "no record" response is communicated to the requesting official.

Article V. Record Request Procedures

(1) Subject fingerprints or other approved forms of positive identification must be submitted with all requests for criminal history record checks for noncriminal justice purposes.



(2) Each request for a criminal history record check utilizing the national indexes made under any approved state statute must be submitted through that state's criminal history record repository. A state criminal history record repository shall process an interstate request for noncriminal justice purposes through the national indexes only if the request is transmitted through another state criminal history record repository or the FBI.

(3) Each request for criminal history record checks utilizing the national indexes made under federal authority must be submitted through the FBI or, if the state criminal history record repository consents to process fingerprint submissions, through the criminal history record repository in the state in which the request originated. Direct access to the national identification index by entities other than the FBI and state criminal history records repositories may not be permitted for noncriminal justice purposes.

(4) A state criminal history record repository or the FBI:

(a) May charge a fee, in accordance with applicable law, for handling a request involving fingerprint processing for noncriminal justice purposes; and

(b) May not charge a fee for providing criminal history records in response to an electronic request for a record that does not involve a request to process fingerprints.

(5) (a) If a state criminal history record repository cannot positively identify the subject of a record request made for noncriminal justice purposes, the request, together with fingerprints or other approved identifying information, must be forwarded to the FBI for a search of the national indexes.

(b) If, with respect to a request forwarded by a state criminal history record repository under subsection (5)(a), the FBI positively identifies the subject as having a III System-indexed record or records:

(i) The FBI shall so advise the state criminal history record repository; and

(ii) The state criminal history record repository is entitled to obtain the additional criminal history record information from the FBI or other state criminal history record repositories.

(Added to NRS by [1999, 771](#))

PENALTIES

NRS 179A.900 Unlawful acts. Any person who:

1. Willfully requests, obtains or seeks to obtain records of criminal history under false pretenses;
2. Willfully communicates or seeks to communicate records of criminal history to any agency or person except pursuant to this chapter; or

3. Willfully falsifies any record of criminal history or any record relating to records of criminal history,

↪ is guilty of a misdemeanor.

(Added to NRS by [1979, 1855](#))

National Crime Prevention and Privacy Compact Council



Security and Management Control Outsourcing Standard for Non-Channelers

Approved by the Council on
May 16, 2018

SECURITY and MANAGEMENT CONTROL OUTSOURCING STANDARD for NON-CHANNELERS

The goal of this document is to provide adequate security and integrity for criminal history record information (CHRI) while under the control or management of an outsourced third party, the Contractor. Adequate security is defined in Office of Management and Budget Circular A-130 as “security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.”

The intent of this Security and Management Control Outsourcing Standard (Outsourcing Standard) is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the FBI Criminal Justice Information Services (CJIS) Security Policy) as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

This Outsourcing Standard identifies the duties and responsibilities with respect to adequate internal controls within the contractual relationship so that the security and integrity of the Interstate Identification Index (III) System and CHRI are not compromised. The standard security program shall include consideration of site security, dissemination restrictions, personnel security, system security, and data security.

The provisions of this Outsourcing Standard are established by the Compact Council pursuant to 28 CFR Part 906 and are subject to the scope of that rule. They apply to all personnel, systems, networks, and facilities supporting and/or acting on behalf of the Authorized Recipient to perform noncriminal justice administrative functions requiring access to CHRI without a direct connection to the FBI CJIS Wide Area Network (WAN).

1.0 *Definitions*

- 1.01 *Access to CHRI* means to view or make use of CHRI obtained from the III System but excludes direct access to the III System by computer terminal or other automated means by Contractors other than those that may be contracted by the FBI or state criminal history record repositories or as provided by Title 34, United States Code (U.S.C.), Section 40314 (b), (formally cited as 42 U.S.C. § 14614(b)).
- 1.02 *Authorized Recipient* means (1) a nongovernmental entity authorized by federal statute or federal executive order to receive CHRI for noncriminal justice purposes, or (2) a government agency authorized by federal statute, federal executive order, or state statute which has been approved by the United States Attorney General to receive CHRI for noncriminal justice purposes.

- 1.03 *Chief Administrator* means the primary administrator of a Nonparty State's criminal history record repository or a designee of such administrator who is a regular full-time employee of the repository, which is also referred to as the State Identification Bureau (SIB) Chief.
- 1.04 *CHRI*, as referred to in Article I(4) of the Compact, means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, or release; but does not include identification information such as fingerprint records if such information does not indicate involvement of the individual with the criminal justice system.
- 1.05 *Criminal History Record Check*, for purposes of this Outsourcing Standard only, means an authorized noncriminal justice fingerprint-based search of a state criminal history record repository and/or the FBI system.
- 1.06 *Compact Officer*, as provided in Article I(2) of the Compact, means (A) with respect to the Federal Government, an official [FBI Compact Officer] so designated by the Director of the FBI [to administer and enforce the compact among federal agencies], or (B) with respect to a Party State, the chief administrator of the State's criminal history record repository or a designee of the chief administrator who is a regular full-time employee of the repository.
- 1.07 *Contractor* means a government agency, a private business, non-profit organization or individual, that is not itself an Authorized Recipient with respect to the particular noncriminal justice purpose, who has entered into a contract with an Authorized Recipient to perform noncriminal justice administrative functions requiring access to CHRI.
- 1.08 *Dissemination* means the disclosure of CHRI by an Authorized Recipient to an authorized Contractor, or by the Contractor to another Authorized Recipient consistent with the Contractor's responsibilities and with limitations imposed by federal and state laws, regulations, and standards as well as rules, procedures, and standards established by the Compact Council and the United States Attorney General.
- 1.09 *Identity History Summary (IdHS)*, for the purposes of this Outsourcing Standard, means the report of all identification, demographic, and event information (criminal and/or civil) within a Next Generation Identification (NGI) Identity record which may be disseminated to an Authorized Recipient contingent upon legislation and federal regulations. The IdHS contains the criminal justice information associated with criminal fingerprint (i.e., "rap sheets") and/or noncriminal justice information associated with the civil fingerprints, therefore the existence of an IdHS

alone does not reflect criminal history events on that NGI Identity. This term is unique to NGI and is not intended to affect other agencies' use of the term "rap sheet" to describe reports of information in their identification repositories.

- 1.10 *Noncriminal Justice Administrative Functions* means the routine noncriminal justice administrative functions relating to the processing of CHRI, to include but not limited to the following:
 - 1. Making fitness determinations/recommendations
 - 2. Obtaining missing dispositions
 - 3. Disseminating CHRI as authorized by Federal statute, Federal Executive Order, or State statute approved by the United States Attorney General
 - 4. Other authorized activities relating to the general handling, use, and storage of CHRI
- 1.11 *Noncriminal Justice Purposes*, as provided in Article I(18) of the Compact, means uses of criminal history records for purposes authorized by federal or state law other than purposes relating to criminal justice activities, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.
- 1.12 *Outsourcing Standard* means a document approved by the Compact Council after consultation with the United States Attorney General which is to be incorporated by reference into a contract between an Authorized Recipient and a Contractor. This Outsourcing Standard authorizes access to CHRI for noncriminal justice purposes, limits the use of the information to the purposes for which it is provided, prohibits retention and/or dissemination except as specifically authorized, ensures the security and confidentiality of the information, provides for audits and sanctions, provides conditions for termination of the contract, and contains such other provisions as the Compact Council may require.
- 1.13 *Personally Identifiable Information (PII)* means information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name.
- 1.14 *Physically Secure Location* means a facility or an area, a room, or a group of rooms, within a facility with both the physical and personnel security controls sufficient to protect CHRI and associated information systems.
- 1.15 *PII Breach* means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access or any similar term referring to situations where persons other than the authorized users, and for other

than authorized purposes, have access or potential access to PII, whether physical or electronic.

- 1.16 *Positive Identification*, as provided in Article I(20) of the Compact, means a determination, based upon a comparison of fingerprints¹ or other equally reliable biometric identification techniques, that the subject of a record search is the same person as the subject of a criminal history record or records indexed in the III System. Identifications based solely upon a comparison of subjects' names or other non-unique identification characteristics or numbers, or combinations thereof, shall not constitute positive identification.
- 1.17 *Public Carrier Network* means a telecommunications infrastructure consisting of network components that are not owned, operated, and managed solely by the agency using that network, i.e., any telecommunications infrastructure which supports public users other than those of the agency using that network. Examples of a public carrier network include but are not limited to the following: Dial-up and Internet connections, network connections to Verizon, network connections to AT&T, ATM Frame Relay clouds, wireless networks, wireless links, and cellular telephones. A public carrier network provides network services to the public; not just to the single agency using that network.
- 1.18 *Security Violation* means the failure to prevent or failure to institute safeguards to prevent access, use, retention, or dissemination of CHRI in violation of: (A) Federal or state law, regulation, or Executive Order; or (B) a rule, procedure, or standard established by the Compact Council and the United States Attorney General.

2.0 *Responsibilities of the Authorized Recipient*

- 2.01 Prior to engaging in outsourcing any noncriminal justice administrative functions, the Authorized Recipient shall: (a) Request and receive written permission from (1) the State Compact Officer/Chief Administrator² or (2)

¹ The Compact Council currently defines positive identification for noncriminal justice purposes as identification based upon a qualifying ten-rolled or qualifying ten-flat fingerprint submission. Further information concerning positive identification may be obtained from the FBI Compact Council office.

²The Compact Officer/Chief Administrator may not grant such permission unless he/she has implemented a combined state/federal audit program to, at a minimum, triennially audit a representative sample of the Contractors and Authorized Recipients engaging in outsourcing with the first of such audits to be conducted within one year of the date the Contractor first receives CHRI under the approved outsourcing agreement. A representative sample will be based on generally accepted statistical sampling methods.

the FBI Compact Officer³; and (b) provide the State Compact Officer/Chief Administrator or the FBI Compact Officer copies of the specific authority for the outsourced work, criminal history record check requirements, and/or a copy of relevant portions of the contract as requested.

- 2.02 The Authorized Recipient shall execute a contract or agreement prior to providing a Contractor access to CHRI. The contract shall, at a minimum, incorporate by reference and have appended thereto this Outsourcing Standard.
- 2.03 The Authorized Recipient shall, in those instances when the Contractor is to perform duties requiring access to CHRI, specify the terms and conditions of such access; limit the use of such information to the purposes for which it is provided; limit retention of the information to a period of time not to exceed that period of time the Authorized Recipient is permitted to retain such information; prohibit dissemination of the information except as specifically authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General; ensure the security and confidentiality of the information to include confirmation that the intended recipient is authorized to receive CHRI; provide for audits and sanctions; provide conditions for termination of the contract; and ensure that Contractor personnel comply with this Outsourcing Standard.
 - a. The Authorized Recipient shall conduct criminal history record checks of Contractor personnel having access to CHRI if such checks of the Authorized Recipient's personnel are required or authorized under an existing federal statute, executive order, or state statute approved by the United States Attorney General under Public Law 92-544.⁴ The Authorized Recipient shall maintain updated records of Contractor personnel who have access to CHRI and update those records within 24 hours when changes to that access

³State or local Authorized Recipients based on State or Federal Statutes shall contact the State Compact Officer/Chief Administrator. Federal or Regulatory Agency Authorized Recipients shall contact the FBI Compact Officer.

⁴If a national criminal history record check of Authorized Recipient personnel having access to CHRI is mandated or authorized by a federal statute, executive order, or state statute approved by the United States Attorney General under Public Law 92-544, the State Compact Officer/Chief Administrator and/or the FBI Compact Officer must ensure Contractor personnel accessing CHRI are either covered by the existing law or that the existing law is amended to include such Contractor personnel prior to authorizing outsourcing initiatives. The national criminal history record checks of Contractor personnel with access to CHRI cannot be outsourced and must be performed by the Authorized Recipient.

- occur and, if a criminal history record check is required, the Authorized Recipient shall maintain a list of Contractor personnel who successfully completed the criminal history record check.
- b. The Authorized Recipient shall ensure that the Contractor maintains site security. (See the current CJIS Security Policy [www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view])
 - c. The State Compact Officer/Chief Administrator or the FBI Compact Officer shall make available the most current versions of both the Outsourcing Standard and the CJIS Security Policy to the Authorized Recipient within 60 calendar days (unless otherwise directed) of notification of successor versions of the Outsourcing Standard and/or the CJIS Security Policy. The Authorized Recipient shall notify the Contractor within 60 calendar days of the FBI/state notification regarding changes or updates to the Outsourcing Standard and/or the CJIS Security Policy. The Authorized Recipient shall be responsible to ensure the most updated versions are incorporated by reference at the time of contract, contract renewal, or within the 60 calendar day notification period, whichever is sooner.
 - d. The Authorized Recipient and/or Contractor shall make available to the State Compact Officer/Chief Administrator or the FBI Compact Officer the relevant portions of the current and approved contract relating to CHRI, upon request.
- 2.04 The Authorized Recipient shall understand the communications and record capabilities of the Contractor which has access to federal or state records through, or because of, its outsourcing relationship with the Authorized Recipient. The Authorized Recipient shall request and approve a topological drawing which depicts the interconnectivity of the Contractor's network configuration as it relates to the outsourced function(s). The Authorized Recipient shall understand and approve any modifications to the Contractor's network configuration as it relates to the outsourced function(s). For approvals granted through the State Compact Officer/Chief Administrator, the Authorized Recipient, if required, shall coordinate the approvals with the State Compact Officer/Chief Administrator.
- 2.05 The Authorized Recipient is responsible for the actions of the Contractor and shall monitor the Contractor's compliance to the terms and conditions of the Outsourcing Standard. For approvals granted through the FBI Compact Officer, the Authorized Recipient shall certify to the FBI Compact Officer that an audit was conducted with the Contractor within 90 days of the date the Contractor first receives CHRI under the approved

outsourcing agreement. For approvals granted through the State Compact Officer/Chief Administrator, the Authorized Recipient, in conjunction with the State Compact Officer/Chief Administrator, will conduct an audit of the Contractor within 90 days of the date the Contractor first receives CHRI under the approved outsourcing agreement. The Authorized Recipient shall certify to the State Compact Officer/Chief Administrator that the audit was conducted.

- 2.06 The Authorized Recipient shall provide written notice of any early voluntary termination of the contract to the Compact Officer/Chief Administrator or the FBI Compact Officer.
- 2.07 The Authorized Recipient shall appoint an Information Security Officer. The Authorized Recipient's Information Security Officer shall:
 - a. Serve as the security POC for the FBI CJIS Division Information Security Officer.
 - b. Document technical compliance with this Outsourcing Standard.
 - c. Establish a security incident response and reporting procedure to discover, investigate, document, and report on major incidents that significantly endanger the security or integrity of the noncriminal justice agency systems to the CJIS Systems Officer, State Compact Officer/Chief Administrator and the FBI CJIS Division Information Security Officer.
- 2.08 The Authorized Recipient shall immediately (within one hour) notify the State Compact Officer/Chief Administrator or the FBI of any PII breach. The Authorized Recipient shall also provide a written report of any PII breach (to include unauthorized access to CHRI by the Contractor) to the State Compact Officer/Chief Administrator or the FBI within five calendar days of receipt of the initial report of the PII breach. The written report must include corrective actions taken by the Authorized Recipient and, if necessary, the Contractor to resolve such PII breach.

3.0 *Responsibilities of the Contractor*

- 3.01 The Contractor and its employees shall comply with all federal and state laws, regulations, and standards (including the CJIS Security Policy) as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.
- 3.02 The Contractor shall develop, document, administer, and maintain a Security Program (Physical, Personnel, and Information Technology) to comply with the most current Outsourcing Standard and the most current CJIS Security Policy. The Security Program shall describe the implementation of the security requirements outlined in this Outsourcing Standard and the CJIS Security Policy. In addition, the Contractor is also

responsible to set, maintain, and enforce the standards for the selection, supervision, and separation of personnel who have access to CHRI. The Authorized Recipient shall provide the written approval to the State Compact Officer/Chief Administrator or the FBI Compact Officer of a Contractor's Security Program. For approvals granted through the State Compact Officer/Chief Administrator, it is the responsibility of the State Compact Officer/Chief Administrator to ensure the Authorized Recipient is in compliance with the CJIS Security Policy.

- 3.03 The requirements for a Security Program should include, at a minimum:
- a) Description of the implementation of the security requirements described in this Outsourcing Standard and the CJIS Security Policy.
 - b) Security Training.
 - c) Guidelines for documentation of security violations to include:
 - i) Develop and maintain a written incident reporting plan to address security events, to include violations and incidents. (See the CJIS Security Policy {[www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/ view](http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view)}).
 - ii) A process in place for reporting security violations.
 - d) Standards for the selection, supervision, and separation of personnel with access to CHRI.
- **If the Contractor is using a corporate policy, it must meet the requirements outlined in this Outsourcing Standard and the CJIS Security Policy. If the corporate policy is not this specific, it must flow down to a level where the documentation supports these requirements.
- 3.04 Except when the training requirement is retained by the Authorized Recipient, the Contractor shall develop a Security Training Program for all Contractor personnel with access to CHRI prior to their appointment/assignment. The Authorized Recipient shall review and provide to the Contractor written approval of the Security Training Program. Training shall be provided upon receipt of notice from the Compact Officer/Chief Administrator on any changes to federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General. Annual refresher training shall also be provided. The Contractor shall annually, not later than the anniversary date of the contract, certify in writing to the Authorized Recipient that annual refresher training was completed for those Contractor personnel with access to CHRI.
- 3.05 The Contractor shall make its facilities available for announced and unannounced audits and security inspections performed by the Authorized Recipient, the state, or the FBI on behalf of the Compact Council.

- 3.06 The Contractor's Security Program is subject to review by the Authorized Recipient, the Compact Officer/Chief Administrator, and the FBI CJIS Division. During this review, provision will be made to update the Security Program to address security violations and to ensure changes in policies and standards as well as changes in federal and state law are incorporated.
 - 3.07 The Contractor shall maintain CHRI only for the period of time necessary to fulfill its contractual obligations but not to exceed the period of time that the Authorized Recipient is authorized to maintain and does maintain the CHRI.
 - 3.08 The Contractor shall maintain a log of any dissemination of CHRI, for a minimum of 365 days.
 - 3.09 The Authorized Recipient and/or Contractor shall make available to the State Compact Officer/Chief Administrator or the FBI Compact Officer the relevant portions of the current and approved contract relating to CHRI, upon request.
- 4.0 *Site Security*
- 4.01 The Authorized Recipient shall ensure that the Contractor site(s) is a physically secure location to protect against any unauthorized access to CHRI.
- 5.0 *Dissemination*
- 5.01 The Contractor shall not disseminate CHRI without the consent of the Authorized Recipient, and as specifically authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.
 - 5.02 An up-to-date log concerning dissemination of CHRI shall be maintained by the Contractor for a minimum one year retention period. This log must clearly identify: (A) the Authorized Recipient with unique identifiers to include the FBI assigned Originating Agency Identifiers to include the FBI assigned Originating Agency Identifier (ORI)/Originating Agency Case (OCA) number, (B) the Transaction Control Number (TCN), (C) the date of dissemination, (D) the statutory authority for dissemination, and (E) the means of dissemination.
 - 5.03 If CHRI is stored or disseminated in an electronic format, the Contractor shall protect against unauthorized access to the equipment and any of the data. In no event shall responses containing CHRI be disseminated other than as governed by this Outsourcing Standard or more stringent contract requirements.

6.0 *Personnel Security*

- 6.01 If a local, state, or federal written standard requires or authorizes a criminal history record check of the Authorized Recipient's personnel with access to CHRI, then a criminal history record check shall be required of the Contractor's (and approved Sub-Contractor's) employees having access to CHRI. Criminal history record checks of Contractor and approved Sub-Contractor employees, at a minimum, will be no less stringent than criminal history record checks that are performed on the Authorized Recipient's personnel performing similar functions. Criminal history record checks must be completed prior to accessing CHRI under the contract.
- 6.02 The Contractor shall ensure that each employee performing work under the contract is aware of the requirements of the Outsourcing Standard and the state and federal laws governing the security and integrity of CHRI. The Contractor shall confirm in writing that each employee has certified in writing that he/she understands the Outsourcing Standard requirements and laws that apply to his/her responsibilities. The Contractor shall maintain the employee certifications in a file that is subject to review during audits. Employees shall make such certification prior to performing work under the contract.
- 6.03 The Contractor shall maintain updated records of personnel who have access to CHRI, update those records within 24 hours when changes to that access occur, and if a criminal history record check is required, maintain a list of personnel who have successfully completed criminal history record checks. The Contractor shall notify Authorized Recipients within 24 hours when additions or deletions occur.

7.0 *System Security*

- 7.01 The Contractor's security system shall comply with the CJIS Security Policy in effect at the time the Outsourcing Standard is incorporated into the contract and with successor versions of the CJIS Security Policy.
 - a. Devices shall be implemented to provide a point of defense and a controlled and audited access to CHRI, both from inside and outside the networks.
 - b. Data encryption shall be required for data in transit pursuant to the requirements in the CJIS Security Policy.
- 7.02 The Contractor shall provide for the secure storage and disposal of all hard copy and media associated with the system to prevent access by unauthorized personnel.

See the current CJIS Security Policy to address: [www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view]

 - a. Physically secure location.

- b. Sanitization procedures for all fixed and non-fixed storage media.
 - c. Storage procedures for all fixed and non-fixed storage media.
- 7.03 To prevent and/or detect unauthorized access to CHRI in transmission or storage, each Authorized Recipient, Contractor, or Sub-Contractor must be assigned a unique identifying number.

8.0 *Security Violations*

8.01 Duties of the Authorized Recipient and Contractor

- a. The Authorized Recipient shall develop and maintain a written policy for discipline of Contractor employees who violate the security provisions of the contract, which includes this Outsourcing Standard that is incorporated by reference. The Authorized Recipient shall develop and maintain a written incident reporting plan for security events, to include violations and incidents. (See also Sections 2.07 and 3.03)
- b. Pending investigation, the Contractor shall, upon detection or awareness, suspend any employee who commits a security violation from assignments in which he/she has access to CHRI under the contract.
- c. The Contractor shall immediately (within one hour of discovery) notify the Authorized Recipient, the State Compact Officer/Chief Administrator, or the FBI of any security violation to include unauthorized access to CHRI. Within five calendar days of such discovery, the Contractor shall provide the Authorized Recipient, the State Compact Officer/Chief Administrator or the FBI a written report documenting such security violation, corrective actions taken by the Contractor to resolve such violation, and the date, time, and summary of the violation.
- d. The Authorized Recipient shall immediately (within four hours) notify the State Compact Officer/Chief Administrator and the FBI Compact Officer of any security violation or termination of the contract, to include unauthorized access to CHRI made available pursuant to the contract. The Authorized Recipient shall provide a written report of any security violation (to include unauthorized access to CHRI by the Contractor) to the State Compact Officer/Chief Administrator, if applicable, and the FBI Compact Officer, within five calendar days of receipt of the written report from the Contractor. The written report must include any corrective actions taken by the Contractor and the Authorized Recipient to resolve such security violation.

- 8.02 Termination of the contract by the Authorized Recipient for security violations
- a. The contract is subject to termination by the Authorized Recipient for security violations involving CHRI obtained pursuant to the contract.
 - b. The contract is subject to termination by the Authorized Recipient for the Contractor's failure to notify the Authorized Recipient of any security violation or to provide a written report concerning such violation.
 - c. If the Contractor refuses to or is incapable of taking corrective actions to successfully resolve a security violation, the Authorized Recipient shall terminate the contract.
- 8.03 Suspension or termination of the exchange of CHRI for security violations
- a. Notwithstanding the actions taken by the State Compact Officer, if the Authorized Recipient fails to provide a written report notifying the State Compact Officer/Chief Administrator or the FBI Compact Officer of a security violation, or refuses to or is incapable of taking corrective action to successfully resolve a security violation, the Compact Council or the United States Attorney General may suspend or terminate the exchange of CHRI with the Authorized Recipient pursuant to 28 CFR §906.2(d).
 - b. If the exchange of CHRI is suspended, it may be reinstated after satisfactory written assurances have been provided to the Compact Council Chairman or the United States Attorney General by the Compact Officer/Chief Administrator, the Authorized Recipient and the Contractor that the security violation has been resolved. If the exchange of CHRI is terminated, the Contractor's records (including media) containing CHRI shall be deleted or returned in accordance with the provisions and time frame as specified by the Authorized Recipient.
- 8.04 The Authorized Recipient and Contractor shall provide written notice (through the State Compact Officer/Chief Administrator if applicable) to the FBI Compact Officer of the following:
- a. The termination of a contract for security violations.
 - b. Security violations involving the unauthorized access to CHRI.
 - c. The Contractor's name and unique identification number, the nature of the security violation, whether the violation was intentional, and the number of times the violation occurred.
- 8.05 The Compact Officer/Chief Administrator, Compact Council and the United States Attorney General reserve the right to investigate or decline to investigate any report of unauthorized access to CHRI.

- 8.06 The Compact Officer/Chief Administrator, Compact Council, and the United States Attorney General reserve the right to audit the Authorized Recipient and the Contractor's operations and procedures at scheduled or unscheduled times. The Compact Council, the United States Attorney General, and the state are authorized to perform a final audit of the Contractor's systems after termination of the contract.

9.0 *PII*

- 9.01 The Contractor is responsible for protecting all PII in its possession and control when handling, using, or storing CHRI.
- 9.02 The Contractor shall notify authorized individuals of their right to report PII breaches directly to the FBI should they believe their information has been mishandled or compromised.
- 9.03 The Contractor shall immediately (within one hour of discovery) notify the Authorized Recipient, the State Compact Officer/Chief Administrator, or the FBI of any PII breach or potential PII breach. Within five calendar days of such discovery, the Contractor shall provide the Authorized Recipient, the State Compact Officer/Chief Administrator, or the FBI a written report documenting such violation and corrective actions taken to resolve such violation, to include the date, time, and summary of the notification to resolve such breach.

10.0 *Miscellaneous Provisions*

- 10.01 This Outsourcing Standard does not confer, grant, or authorize any rights, privileges, or obligations to any persons other than the Contractor, the Authorized Recipient, Compact Officer/Chief Administrator (where applicable), and the FBI.
- 10.02 The following document is incorporated by reference and made part of this Outsourcing Standard: (1) The CJIS Security Policy.
- 10.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they provide a minimum basis for the security of the system and the CHRI accessed therefrom and it is understood that there may be terms and conditions of the appended contract which impose more stringent requirements upon the Contractor.⁵

⁵Such conditions could include additional audits, fees, or security requirements. The Compact Council, Authorized Recipients, and the Compact Officer/Chief Administrator have the explicit authority to require more stringent standards than those contained in the Outsourcing Standard.

- 10.04 The minimum security measures as outlined in this Outsourcing Standard may only be modified by the Compact Council. Conformance to such security measures may not be less stringent than stated in this Outsourcing Standard without the consent of the Compact Council in consultation with the United States Attorney General.
- 10.05 This Outsourcing Standard may only be modified by the Compact Council and may not be modified by the parties to the appended contract without the consent of the Compact Council.
- 10.06 Appropriate notices, assurances, and correspondence to the FBI Compact Officer, Compact Council, and the United States Attorney General required by Section 8.0 of this Outsourcing Standard shall be forwarded by First Class Mail to:
- FBI Compact Officer
1000 Custer Hollow Road
Module D-3
Clarksburg, WV 26306

11.0 *Exemption from Above Provisions*

- 11.01 An Information Technology (IT) contract need only include Sections 1.0, 2.01, 2.02, 2.03, 3.01, 6.0, 8.0, and 9.0 of this Outsourcing Standard for Non-Channelers when all of the following conditions exist:

1. Access to CHRI by the IT contractor's personnel is limited solely for the development and/or maintenance of the Authorized Recipient's computer system;
2. Access to CHRI is incidental, but necessary, to the duties being performed by the IT contractor;
3. The computer system resides within the Authorized Recipient's facility;
4. The Authorized Recipient's personnel supervise or work directly with the IT contractor personnel;
5. The Authorized Recipient maintains complete, positive control of the IT contractor's access to the computer system and CHRI contained therein; and
6. The Authorized Recipient retains all of the duties and responsibilities for the performance of its authorized noncriminal justice administrative functions, unless it executes a separate contract to perform such noncriminal justice administrative functions, subject to all applicable requirements, including the Outsourcing Standard.

- 11.02 An Authorized Recipient's contract where access to CHRI is limited solely for the purposes of: (A) storage (referred to as archiving in some states) of

the CHRI at the Contractor's facility; (B) retrieval of the CHRI by Contractor personnel on behalf of the Authorized Recipient with appropriate security measures in place to protect the CHRI; and/or (C) destruction of the CHRI by Contractor personnel when not observed by the Authorized Recipient need only include Sections 1.0, 2.01, 2.02, 2.03, 3.01, 4.0, 6.0, 8.0, and 9.0 of this Outsourcing Standard for Non-Channelers when all of the following conditions exist:

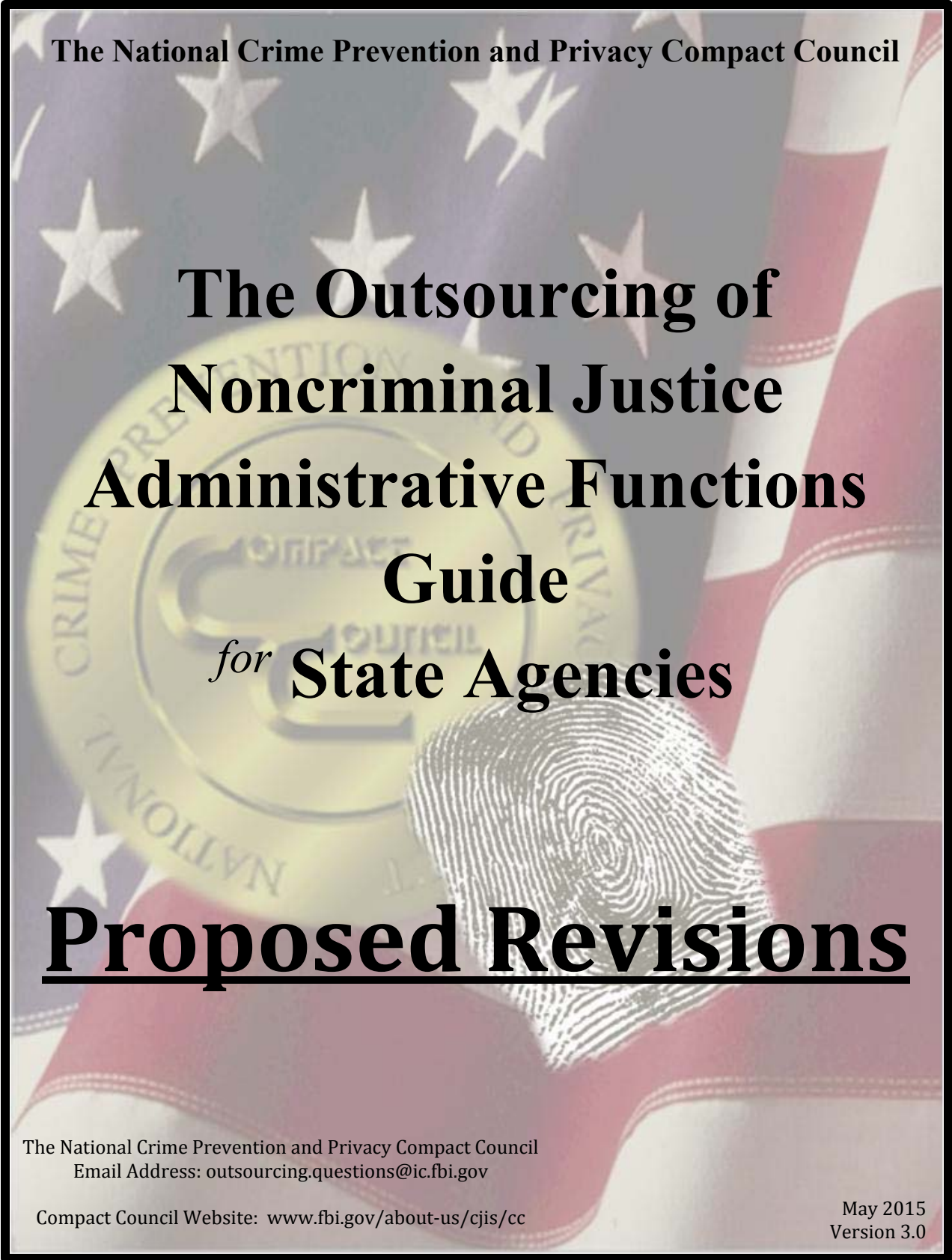
1. Access to CHRI by the Contractor is limited solely for the purposes of: (A) storage (referred to as archiving in some states) of the CHRI at the Contractor's facility; (B) retrieval of the CHRI by Contractor personnel on behalf of the Authorized Recipient with appropriate security measures in place to protect the CHRI; and/or (C) destruction of the CHRI by Contractor personnel when not observed by the Authorized Recipient;
2. Access to CHRI is incidental, but necessary, to the duties being performed by the Contractor;
3. The Contractor is not authorized to disseminate CHRI to any other agency or contractor on behalf of the Authorized Recipient;
4. The Contractor's personnel are subject to the same criminal history record checks as the Authorized Recipient's personnel;
5. The criminal history record checks of the Contractor personnel are completed prior to work on the contract or agreement;
6. The Authorized Recipient retains all other duties and responsibilities for the performance of its authorized noncriminal justice administrative functions, unless it executes a separate contract to perform such noncriminal justice administrative functions, subject to all applicable requirements, including the Outsourcing Standard; and
7. The Contractor stores the CHRI in a physically secure location.

12.0 *Duties of the State Compact Officer/Chief Administrator*

- 12.01 The State Compact Officer/Chief Administrator shall review legal authority and respond in writing to the Authorized Recipient's request to outsource noncriminal justice administrative functions.
- 12.02 The State Compact Officer/Chief Administrator reserves the right to review relevant portions of the outsourcing contract relating to CHRI throughout the duration of the contract approval.

- 12.03 The State Compact Officer/Chief Administrator must ensure criminal history record checks on approved Contractor and Sub-Contractor employees with access to CHRI are completed by the Authorized Recipient, if such checks are required or authorized of the Authorized Recipient personnel by federal statute, executive order, or state statute approved by the United States Attorney General under Public Law 92-544. Criminal history record checks should be no less stringent than the checks performed on the Authorized Recipient personnel. Criminal history record checks must be completed prior to accessing CHRI under the contract.
- 12.04 Coordinate with the Authorized Recipient for the review and approval of the Contractor's Topological drawing which depicts the interconnectivity of the Contractor's network configuration as it relates to the outsourcing function(s).
- 12.05 90 Day Compliance Review
- a. The State Compact Officer/Chief Administrator shall work in coordination with the Authorized Recipient to conduct an audit of the Contractor within 90 days of the date the Contractor first receives CHRI under the approved outsourcing agreement.
 - b. The State Compact Officer/Chief Administrator shall review the Authorized Recipient's audit certification to ensure compliance with the Outsourcing Standard.
 - i) The State Compact Officer/Chief Administrator shall address concerns with the Authorized Recipient resulting in non-compliance with the 90 day audit of the Contractor.
 - ii) The State Compact Officer/Chief Administrator shall have the right to terminate an Authorized Recipient's Outsourcing approval to a Contractor(s) for failure or refusal to correct a non-compliance issue(s).
- 12.06 The State Compact Officer/Chief Administrator shall coordinate with the Authorized Recipient to review the Contractor's Security Program. The program shall describe the implementation of the security requirements outlined in this Outsourcing Standard and the CJIS Security Policy. During the review, provisions will be made to update the Security Program to address security events and to ensure changes in policies and standards, as well as changes in federal and state law, are incorporated.
- 12.07 The State Compact Officer/Chief Administrator shall audit the Authorized Recipient and/or Contractor's operations and procedures. This may be done at scheduled and unscheduled times.
- 12.08 The State Compact Officer/Chief Administrator shall assign a unique identifying number to each Authorized Recipient, Contractor, or Sub-Contractor to ensure system security.

- 12.09 The State Compact Officer/Chief Administrator shall require immediate (within four hours) notification by the Authorized Recipient of any security event, to include security violations and incidents or termination of the contract, to include unauthorized access to CHRI made available pursuant to the contract. The State Compact Officer/Chief Administrator shall receive a written report from the Authorized Recipient of any security event (to include unauthorized access to CHRI by the Contractor) within five calendar days of receipt of the written report from the Contractor, that must include any corrective actions taken by the Contractor and Authorized Recipient to resolve such security event. (See the CJIS Security Policy {www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view})
- 12.10 Suspension or termination of the exchange of CHRI for security events.
- a. The State Compact Officer/Chief Administrator may suspend or terminate the exchange of CHRI for security events or refusal or incapability to take corrective action to successfully resolve a security event.
 - b. The State Compact Officer/Chief Administrator may reinstate access to CHRI between the Authorized Recipient and the Contractor after receiving written assurance(s) of corrective action(s) from the Authorized Recipient and/or the Contractor.
- 12.11 The State Compact Officer/Chief Administrator shall provide written notification to the FBI Compact Officer of the termination of a contract for security events to include the security events involving access to CHRI; the Contractor's name and unique identification number; the nature of the security event; whether the event was intentional; and the number of times the event occurred.
- 12.12 The State Compact Officer/Chief Administrator reserves the right to investigate or decline to investigate any report of unauthorized access to CHRI.
- 12.13 The State Compact Officer/Chief Administrator is authorized to perform a final audit of the Contractor's system following termination of contract.



The National Crime Prevention and Privacy Compact Council

**The Outsourcing of
Noncriminal Justice
Administrative Functions
Guide
for State Agencies**

Proposed Revisions

The National Crime Prevention and Privacy Compact Council
Email Address: outsourcing.questions@ic.fbi.gov

Compact Council Website: www.fbi.gov/about-us/cjis/cc

May 2015
Version 3.0

Table of Contents

Introduction.....	3
Background.....	4
Outsourcing: Non-Channeling versus Channeling.....	5
Outsourcing Scenarios	8
Non-Channeling: Outsourcing Fitness Determinations/Recommendations	8
Channeling: Fingerprint Submissions/Results/Dissemination	8
Responsibility Table for Non-Channeling	9
Responsibility Table for Channeling.....	25
Authorized Recipient’s Responsibilities.....	37
Examples of Non-Channeling Documentation	38
Sample Authorized Recipient Request Letter for Non-Channeling	38
Sample Language between the Authorized Recipient and Contractor regarding Noncriminal Justice Outsourcing Functions for Non-Channeling	39
Examples of Channeling Documentation.....	40
Authorized Recipient Sample Request Letter to Use a Channeler	40
Sample FBI Response Letter for Channeler Request	41
Sample Language between the Authorized Recipient and Channeler regarding Noncriminal Justice Outsourcing Functions.....	42
Outsourcing Audit Guidelines.....	43
Sample Audit Methodology	43
Sample 90 day Audit Checklist for an Authorized Recipient.....	45
Non-Channeling Flowchart for SCO/CA	48
Non-Channeling Checklist for SCO/CA	49
Channeling Flowchart for SCO/CA.....	50
Channeling Checklist for SCO/CA.....	51
Frequently Asked Questions.....	52
Recommended Online Reference Materials	54
Definitions	55
Appendices	59
Interim Final Rule: Outsourcing of Noncriminal Justice Administrative Functions.....	60
Final Rule: Outsourcing of Noncriminal Justice Administrative Functions.....	64

Security and Management Control Outsourcing Standard for Channelers.....66

Security and Management Control
Outsourcing Standard for Non-Channelers.....80

Introduction

Noncriminal justice outsourcing incorporates the process of a third party contractor to perform noncriminal justice administrative functions (i.e. making fitness determinations/recommendations, obtaining missing dispositions, archival and off-site storage of fingerprint submissions and corresponding criminal history record results, or the submission of fingerprints and the receipt of corresponding criminal history records) related to the processing of criminal history record information (CHRI) maintained in the Interstate Identification Index (III) System, subject to appropriate controls, when acting on behalf of the governmental or authorized agency. The III is the system of federal and state criminal history records maintained by the Federal Bureau of Investigation (FBI).

The Outsourcing of Noncriminal Justice Administrative Functions Guide for State Agencies (State Guide) was developed by the National Crime Prevention and Privacy Compact Council (Council) in consultation with the FBI's Criminal Justice Information Services (CJIS) Division. The State Guide is designed to provide resources to **state agencies** that engage in and authorize the outsourcing of noncriminal justice administrative functions. The information contained in the State Guide may be used as a resource. States are encouraged to continue to build upon this information to enhance its outsourcing program. Federal or regulatory agencies should contact the FBI Compact Officer for information pertaining to the outsourcing of noncriminal justice administrative functions.

The State Guide is broken down into several sections. Topics include an outline of responsibilities for engaging in a contract or agreement for Non-Channeling and Channeling; samples of contract language and outsourcing requests; audit methodologies; and a variety of checklists. The State Guide also contains a list of frequently asked questions, common definitions relating to the outsourcing of noncriminal justice administrative functions, and additional on-line resources.

Background

The National Crime Prevention and Privacy Compact Act of 1998 (Compact) ((Title 34, United States Code [U.S.C.], Sections 40311 – 40316 (formerly cited as Title 42, U.S.C., Sections 14611-14616)) provides a legal framework for the cooperative exchange of criminal history records between federal and state entities for noncriminal justice purposes. The Compact was signed by President Clinton on October 9, 1998, and became effective on April 28, 1999, when ratified by two states. As of December 2014, 30 states and the federal government have ratified the Compact. States that have ratified the Compact are referred to as “party states.”

The Compact established a fifteen-member Council, whose members are appointed by the United States (U.S.) Attorney General (AG), to promulgate rules, procedures, and standards governing the use of the III System and CHRI for noncriminal justice purposes and to ensure the protection of an individual’s privacy while facilitating the nationwide automated exchange of CHRI. Pursuant to the Compact, each party state is required to appoint a State Compact Officer (SCO) who shall ensure that the Compact provisions, rules, procedures, and standards established by the Council are complied with in his/her respective state.

The Council published the "Outsourcing of Noncriminal Justice Administrative Functions" Interim Final Rule (IFR) and two "Security and Management Control Outsourcing Standards" (Outsourcing Standards) in the *Federal Register* on December 16, 2004. The IFR is attached as *Appendix A*. The Council adopted the IFR as a Final Rule (Rule) and published a combined Outsourcing Standard in the FR on December 15, 2005, which is attached as *Appendix B*. The Rule permits an Authorized Recipient (AR) of CHRI to outsource noncriminal justice administrative functions relating to the processing of CHRI to a third party, subject to appropriate controls.

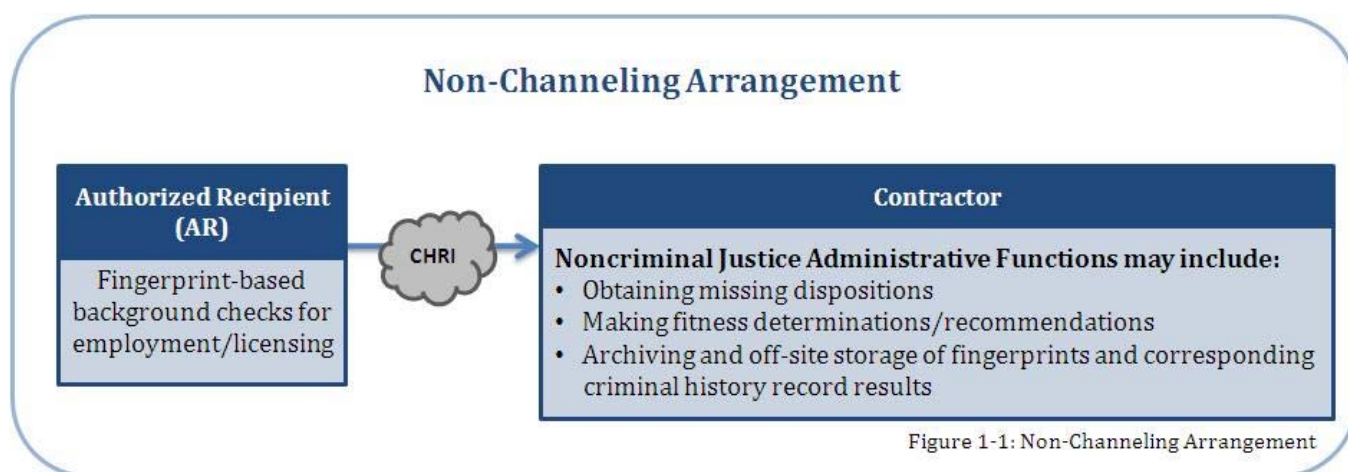
The Outsourcing Standard established minimum requirements to ensure that security and privacy controls are in place when conducting national criminal history record checks for noncriminal justice purposes. The contracting parties may not reduce these minimum standards; however, more restrictive requirements may be adopted by the contracting parties. Additionally, the Outsourcing Standard identified responsibilities for adequate security controls between the AR and the Contractor in order to maintain the security and integrity of the III System and CHRI. The security program shall address site security, dissemination restrictions, personnel security, system security, and guidelines for documentation of security events.

To ensure agencies follow the minimum standards, the Rule states that contracts or agreements providing for authorized outsourcing "shall incorporate by reference a security and management control outsourcing standard approved by the Compact Council after consultation with the United States Attorney General." In November 2009, to clarify the roles, the Council bifurcated the Outsourcing Standard to create one strictly for Channeling (Outsourcing Standard for Channelers) [*Appendix C*] and the other for Non-Channeling (Outsourcing Standard for Non-Channelers) [*Appendix D*]. The Council periodically updates the Outsourcing Standards and the most current versions may be found on the web at <www.fbi.gov/about-us/cjis/cc>.

Outsourcing: Non-Channeling versus Channeling

There are two very separate and distinct parts to the outsourcing of noncriminal justice administrative functions associated with national criminal history records. The first is Non-Channeling. In this scenario, the Contractor receives access to the CHRI directly from the AR. The AR may engage the Contractor to perform a variety of noncriminal justice administrative functions, such as, but not limited to, obtaining missing dispositions, making fitness determinations/recommendations, or the off-site storage and archival of fingerprint submissions and corresponding criminal history record results. In this arrangement, the Contractors do not have a direct connection to the FBI's CJIS Wide Area Network (WAN). The AR provides the results of the national criminal history record check directly to the Contractor. The Contractor performs the desired noncriminal justice administrative function(s). Figure 1-1 depicts a Non-Channeling arrangement.

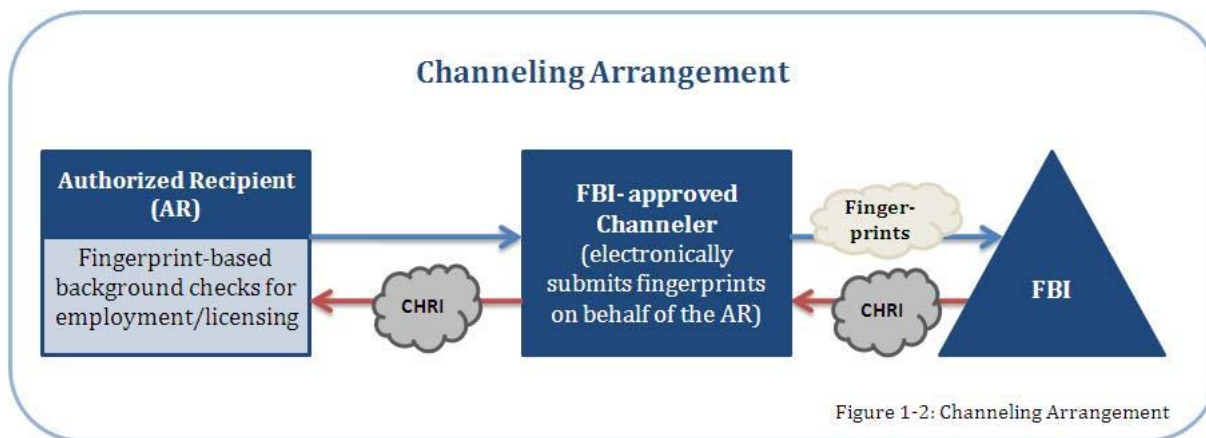
It is important to note that in order to fully comply with footnote 4 of the Outsourcing Standard for Non-Channelers, which provides that if a national criminal history record check of government personnel having access to CHRI is mandated or authorized by a state statute approved by the U.S. AG under Public Law (Pub. L.) 92-544, the SCO or Chief Administrator (CA) of non-party states must ensure Contractor personnel accessing CHRI are either covered by existing law or that the existing law be amended to include national criminal history record checks for Contractors prior to authorizing the outsourcing initiatives. For example, if North Carolina has a statute that permits its governmental and contracted employees who perform only noncriminal justice administrative functions to be backgrounded, then the AR requesting the outsourcing will be required to background the Contractor's employees having access to FBI-provided CHRI while performing noncriminal justice administrative functions. Whereas, if California has enacted a statute that only authorizes the backgrounding of its governmental employees performing only noncriminal justice administrative functions, then the outsourcing approval will not be granted until such authority to background the contracted employees is in place.



The other part of noncriminal justice outsourcing is Channeling, which creates a conduit for an AR to submit fingerprints via an FBI-approved Channeler directly to the FBI, the Channeler receives the CHRI on behalf of the AR, and promptly distributes the CHRI to the AR. The Channeler is a Contractor that has a direct connection to the FBI's CJIS WAN for the electronic submission of fingerprints on behalf of the AR. The FBI electronically returns the corresponding results of each fingerprint-based national criminal history record check to the Channeler and the Channeler expeditiously disseminates the criminal history record check results to the AR. Figure 1-2 illustrates the Channeling arrangement.

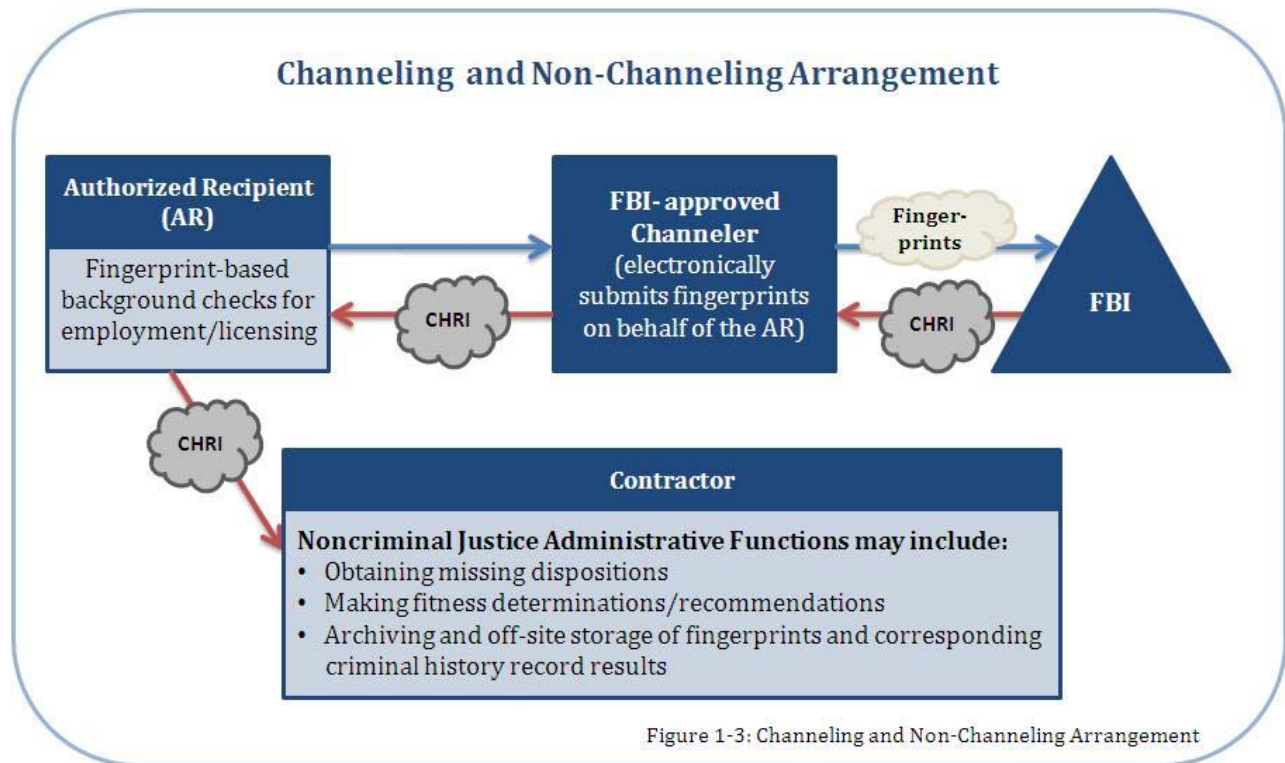
In 2011, the FBI released a Request for Proposal (RFP) to solicit Contractors to provide processing services for authorized national noncriminal justice fingerprint submissions from ARs. In response to the RFP, the FBI selected multiple Contractors to act as Channelers. For a current list of FBI-approved Channelers, visit <www.fbi.gov/about-us/cjis/cc/current-initiatives/list-of-fbi-approved-channelers> or contact the FBI Compact Office at <outsourcing.questions@ic.fbi.gov>. Pursuant to the Outsourcing Standard for Channelers, the FBI is required to conduct criminal history record checks of Channeling personnel having access to CHRI. Thus, in this arrangement, the AR is not responsible for conducting background checks of the Contractor's personnel having access to CHRI.

As a matter of information, if the Contractor is posting national criminal history record check results to a web site, the FBI CJIS Division's Information Security Officer must review and approve the proposed technical configuration prior to the FBI Compact Officer's decision to approve the request.



It is possible for the same Contractor to provide both Channeling and Non-Channeling noncriminal justice administrative functions. If this occurs, there must be a distinct separation between the Channeling and the performance of the other noncriminal justice administrative functions (Non-Channeling). A Channeler must promptly forward the criminal history record check results to the AR, which ends the "Channeling" outsourcing process. Then, the AR would be responsible for selecting and forwarding the criminal history record check results back to the Contractor for the performance of approved Non-Channeling noncriminal justice administrative functions, such as obtaining missing dispositions, outsourced by the AR in compliance with the Outsourcing Standard for Non-Channelers. Such procedures will establish a distinct beginning and end to each of the

outsourcing contracts (i.e., a contract for Channeling and a contract for other noncriminal justice administrative functions). Additionally, this process will facilitate an efficient audit process. Essentially, a Channeler is an “expediter” or “conduit” rather than a user of criminal history record results. The Contractor providing the Non-Channeling function is the user of the information. Figure 1-3 displays the same Contractor performing both the Channeling and Non-Channeling functions.



Outsourcing Scenarios

Non-Channeling: Outsourcing Fitness Determinations/Recommendations

New Hampshire (NH), a party-state, enacts a Pub. L. 92-544 statute that authorizes the state to conduct fingerprint-based background checks on prospective foster parents. The NH Department of Health and Human Services (DHHS) submits a written request to the SCO (or the CA of the State Criminal History Repository for non-party states) to outsource noncriminal justice administrative functions to a Contractor. The specific function that will be outsourced to the Contractor is making fitness determinations/recommendations using the applicant's criminal history information. A sample Non-Channeling request letter may be found under the Examples of Non-Channeling Documentation section.

Upon written approval by the SCO (or the CA), the NH DHHS, as the AR, may utilize a Contractor to perform the specific noncriminal justice administrative function. Therefore, in this instance, upon execution of the necessary outsourcing agreements by the NH DHHS and the Contractor, the NH DHHS may use a Contractor to make fitness determinations/recommendations.

Channeling: Fingerprint Submissions/Results/Dissemination

Wisconsin (WI), a non-party state, enacts a Pub. L. 92-544 statute that authorizes the state to conduct fingerprint-based background checks on licensed health care professionals and unlicensed health care facility personnel. The WI Department of Children and Families (DCF) submits a written request to the CA at the WI State Criminal History Repository (or SCO in a party state) to use an FBI-approved Channeler to perform noncriminal justice functions. The specific functions that the Channeler will perform are submitting fingerprints to the FBI, receiving CHRI on behalf of the DCF, and expeditiously providing the CHRI to the DCF. A sample Channeling request letter may be found under the Examples of Channeling Documentation section.

The CA at the WI State Criminal History Repository (or the SCO) submits a written request to the FBI Compact Officer to outsource the DCF's fingerprint submissions for a national background check to an FBI-approved Channeler. Upon written approval by the FBI Compact Officer, the DCF may utilize an FBI-approved Channeler to perform specific noncriminal justice administrative functions. Therefore, in this instance, upon execution of the necessary outsourcing agreements among the WI State Criminal History Repository, the Channeling Contractor, and the WI DCF, the DCF may use an FBI-approved Channeler to submit fingerprints to the FBI, receive CHRI on behalf of and expeditiously provide the CHRI to the DCF.

Disclaimer: The states and agencies used in the example scenarios were randomly selected.

Responsibility Table for Non-Channeling

Security and Management Control Outsourcing Standard (OS) for Non-Channelers

OS dated 11/06/2014, table updated 12/17/2014

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	State Compact Officer (SCO); FBI Compact Officer (FBI CO); Chief Administrator (CA); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
Section 2.0 - Responsibilities of the AR				
2.01 - Outsourcing Request (See Section 11.01) Footnote 2 - Audit Requirements Footnote 3 - Outsourcing Approval	AR shall: (1) If State or Local AR's based on State or Federal Statutes, request and receive permission from SCO/CA. (2) Provide the SCO/CA copies of the specific authority for the outsourced work, criminal history record check requirements, and/or a copy of relevant portions of the contract as requested.		(1) SCO/CA shall approve/disapprove request in writing. (2) SCO/CA may not grant such permission unless he/she has implemented a combined state/federal audit program to, at a minimum, triennially audit a representative sample of the Contractors and ARs engaging in outsourcing with the first of such audits to be conducted within one year of the date the Contractor first receives CHRI under the approved outsourcing agreement. (3) SCO/CA will review copies of the specific authority for the outsourced work, criminal history record check requirements, and/or a copy of relevant portions of the contract if requested.	
2.02 - Contract 2.03(c) & 7.01 & 9.02 - OS and CJIS Security Policy	AR shall: (1) Execute contract or agreement prior to providing a Contractor access to CHRI. (2) Ensure the most updated versions are incorporated by reference at the time of contract, contract renewal, or within the 60 calendar day notification period, whichever is sooner. (3) Notify the Contractor within 60 calendar days (unless otherwise directed) of FBI notification regarding changes or updates to the OS and/or <i>CJIS Security Policy</i> .	(1) Ensure that the most current version of both the OS and the <i>CJIS Security Policy</i> are incorporated by reference at the time of the contract, contract renewal, or within 60 calendar days (unless otherwise directed) of notification of successor versions of the OS and/or <i>CJIS Security Policy</i> , whichever is sooner.	(1) SCO/CA shall make available the most current version of both the OS and the <i>CJIS Security Policy</i> to the AR within 60 calendar days (unless otherwise directed) of notification of successor versions, whichever is sooner.	

Responsibility Table for Non-Channeling

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	State Compact Officer (SCO); FBI Compact Officer (FBI CO); Chief Administrator (CA); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
2.03 - Access to CHRI	<p>When Contractor will have access to CHRI, the AR shall:</p> <p>(1) Specify terms and conditions of access.</p> <p>(2) Limit the use of the information to the purposes for which provided.</p> <p>(3) Limit the retention of the information to a period of time not to exceed that period of time the AR is permitted to retain such information.</p> <p>(4) Prohibit dissemination except as authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the CC and the US AG.</p> <p>(5) Ensure security and confidentiality of the information to include confirmation that the intended recipient is authorized to receive CHRI.</p> <p>(6) Provide for audits and sanctions.</p> <p>(7) Provide conditions for termination of the contract.</p> <p>(8) Ensure Contractor personnel comply with OS.</p>			
2.03(a) & Footnote 4 - Criminal History Record (CHR) Checks (See Section 11.03)	<p>(1) Conduct criminal history record checks of Contractor personnel having access to CHRI if such checks of the AR's personnel are required or authorized under an existing state statute approved by the U.S. AG under Pub. L. 92-544, federal statute or Executive Order.</p> <p>(2) Maintain updated records of Contractor personnel who have access to CHRI and update those records within 24 hours when changes to that access occur, and if a criminal history record check is required, maintain a list of Contractor personnel who successfully completed the criminal history record check.</p> <p>(3) The national criminal history record checks of Contractor personnel with access to CHRI cannot be</p>		<p>(1) SCO/CA process criminal history record check of Contractor personnel having access to CHRI if such checks are required or authorized of AR's personnel having similar access.</p> <p>(2) If a national criminal history record checks of AR personnel having access to CHRI is mandated or authorized by a federal statute, executive order, or state statute approved by the U.S. AG under Public Law 92-544, the SCO/CA and/or the FBI CO must ensure Contractor personnel accessing CHRI are either covered by the existing law or that the existing law is amended to include such Contractor personnel prior to authorizing outsourcing initiatives.</p>	

Responsibility Table for Non-Channeling

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	State Compact Officer (SCO); FBI Compact Officer (FBI CO); Chief Administrator (CA); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
	outsourced and must be performed by the AR.			
2.03(b) - Site Security See CJIS Security Policy	(1) Ensure Contractor maintains site(s) security.	(1) Maintain site(s) security.		
2.03(c) - See 2.02 - OS & CJIS Security Policy	See 2.02	See 2.02	See 2.02	See 2.02
2.03(d) - Access to Contract (See Section 11.02)	(1) Make available to the SCO/CA the relevant portions of the current and approved contract relating to CHRI, upon request.	(1) Make available to the SCO/CA the relevant portions of the current and approved contract relating to CHRI, upon request.	See 11.02	
2.04 – Records and Topological Drawings (See Section 11.04)	(1) Understand the communications and record capabilities of the Contractor which has access to federal or state records through, or because of, its outsourcing relationship with the AR. (2) Request and approve a topological drawing which depicts the interconnectivity of the Contractor's network configuration as it relates to the outsourced functions. (3) The AR, if required, shall coordinate the approvals with the SCO/CA.	(1) Provide updated topological drawings to AR.	(1) The SCO/CA shall approve a topological drawing which depicts the interconnectivity of the Contractor's network configuration as it relates to the outsourced functions.	
2.05 - 90 Day Compliance Review (See Section 11.05)	(1) Responsible for the actions of Contractor and monitoring the Contractor's compliance to the terms and conditions of the OS. (2) The AR in conjunction with the SCO/CA will conduct an audit of the Contractor within 90 days of the date the Contractor first receives CHRI under the approved outsourcing agreement. The AR shall certify to the SCO/CA that the audit was conducted.		(1) The SCO/CA will review and maintain AR's certification for completion of 90 day compliance review..	
2.06 – Contract Termination (See Section 8.02)	(1) Provide written notice of any early voluntary termination of contract to the SCO/CA.			
2.07 ISO Appointment	(1) Appoint an Information Security Officer (ISO) to: (a) Serve as the security POC for the FBI CJIS Division ISO; (b) Document technical compliance with the OS; and			

Responsibility Table for Non-Channeling

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	State Compact Officer (SCO); FBI Compact Officer (FBI CO); Chief Administrator (CA); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
	(c) Establish a security incident response and reporting procedure to discover, investigate, document, and report on major incidents that significantly endanger the security or integrity of the NCJ agency systems to the CJIS Systems Officer and the FBI CJIS Division ISO.			
3.0 - Responsibilities of the Contractor				
3.01 - Regulation Compliance		(1) Comply with all federal and state laws, regulations, and standards (including the <i>CJIS Security Policy</i>) as well as with rules, procedures, and standards established by the CC and the US AG.		
3.02 - Security Program	(1) Review and provide written approval/disapproval of the Contractor's Security Program to the SCO/CA.	<p>(1) The Contractor shall develop, document, administer, and maintain a Security Program (Physical, Personnel, and IT) to comply with the most current OS and most current <i>CJIS Security Policy</i>.</p> <p>(2) The Security Program shall describe the implementation of the security requirements outlined in this OS and the <i>CJIS Security Policy</i>.</p> <p>(3) Responsible to set, maintain, and enforce the standards for selection, supervision, and separation of personnel who have access to CHRI.</p>	(1) The SCO/CA to ensure the AR is in compliance with the <i>CJIS Security Policy</i> .	
3.03 - Security Requirements See CJIS Security Policy	(1) Review and provide written approval/ disapproval of the Contractor's Security Program.	<p>Requirements for a Security Program should include, at a minimum:</p> <p>(a) Description of the implementation of the security requirements described in the OS and the <i>CJIS Security Policy</i>.</p> <p>(b) Security training.</p> <p>(c) Guidelines for documentation of security violations to include:</p> <p>(i) Develop and maintain a written security incident reporting plan to address security events, to include violations and incidents.</p>		

Responsibility Table for Non-Channeling

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	State Compact Officer (SCO); FBI Compact Officer (FBI CO); Chief Administrator (CA); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
		<p>(ii) Have a process in place for reporting security violations.</p> <p>(d) Standards for the selection, supervision, and separation of personnel with access to CHRI.</p> <p>*If using a corporate policy, it must meet the requirements outlined in the OS and the <i>CJIS Security Policy</i>. If the corporate policy is not this specific, it must flow down to a level where the documentation supports these requirements.</p>		
Section 3.04 – Security Training Program	<p>(1) Review and provide to the Contractor written approval/disapproval of the Contractors Security Training Program.</p> <p>If training requirement is retained by AR:</p> <p>(1) Develop a Security Training Program for all Contractor personnel with access to CHRI prior to their appointment/assignment.</p> <p>(2) Provide training prior to appointment/assignment and upon receipt of notice from the SCO/CA on any changes to federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the CC and the US AG.</p> <p>(3) Provide annual refresher training, not later than the anniversary date of the contract, may certify in writing to the FBI that annual refresher training was completed for those Contractor personnel with access to CHRI.</p>	<p>(1) Except when the training requirement is retained by the AR, Contractor shall develop a Security Training Program for all Contractor personnel with access to CHRI prior to their appointment/ assignment.</p> <p>(2) Provide training upon receipt of notice from the SCO/CA on any changes to federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the CC and the US AG.</p> <p>(3) Provide annual refresher training, not later than the anniversary date of the contract, certify in writing to the AR that annual refresher training was completed for those Contractor personnel with access to CHRI.</p>		
3.05 - Security Inspection (See Section 11.07)	(1) Perform announced and unannounced audits and security inspections.	(1) Make its facilities available for announced and unannounced audits and security inspections performed by the AR, the state, or the FBI on behalf of the CC.	(1) State may perform announced and unannounced audits and security inspections.	(1) FBI on behalf of CC may perform announced and unannounced audits and security inspections.
3.06 – Security Program Review	(1) Review and approve Contractor’s Security Program.	(1) Contractor’s Security Program is subject to	(1) May review Contractor’s Security Program.	(1) May review Contractor’s Security Program.

Responsibility Table for Non-Channeling

Outsourcing Guide for State Agencies					ion (CJIS); ncil (CC);
Outsourcing (OS) Section #	Authorized Recipient (AR)	Contractor	Chief Administrator (CA); CJIS Systems Agency (CSA)	United States Attorney General (US AG)	
(See Sections 3.02 & 11.06)		review by the AR, SCO/CA, FBI CO, and CJIS. (2) During this review, provisions will be made to update the Security Program to address security violations and to ensure changes in policies and standards as well as changes in federal and state law are incorporated.			
3.07 - Maintenance of CHRI		(1) Maintain CHRI only for period of time necessary to fulfill its contractual obligations but not to exceed the period of time that the AR is authorized to maintain and does maintain the CHRI.			
3.08 - CHRI Logging		(1) Maintain log of any dissemination of CHRI for a minimum of 365 days.			
4.0 - Site Security					
4.01 - Physically Secure Location	(1) Ensure Contractor site(s) is a physically secure location to protect against any unauthorized access to CHRI.	(1) Ensure site(s) is a physically secure location to protect against any unauthorized access to CHRI.			
5.0 - Dissemination					
5.01 - Dissemination Authority	(1) Authorize any dissemination of CHRI by the Contractor to ensure that the dissemination falls within the guidelines of federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the CC and the US AG.	(1) Ensure CHRI is not disseminated without the consent of the AR, and as specifically authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the CC and the US AG.			
5.02 - Dissemination Log		(1) Maintain an up-to-date log concerning dissemination of CHRI for a minimum of one year. (2) Log must identify: (a) The AR and the secondary recipient with unique identifiers, (b) the record disseminated, (c) the date of dissemination, (d) the statutory authority for dissemination, and (e) the means of dissemination.			

Responsibility Table for Non-Channeling

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	State Compact Officer (SCO); FBI Compact Officer (FBI CO); Chief Administrator (CA); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
5.03 – Unauthorized Access	(1) Ensure any dissemination of CHRI data by the Contractor is for official purposes only.	(1) If CHRI is stored or disseminated in an electronic format, the Contractor shall protect against unauthorized access to the equipment and any of the data. (2) In no event shall responses containing CHRI be disseminated other than as governed by this OS or more stringent contract requirements.		
6.0 - Personnel Security				
6.01 - Personnel CHR Check (See Section 11.03)	(1) Process CHR checks on Contractor (and approved Sub-Contractor) personnel having unescorted access to CHRI if a local, state, or federal written standard requires or authorizes a CHR check. (2) CHR checks of Contractor (and approved Sub-Contractor) personnel, at a minimum, will be no less stringent than CHR checks that are performed on the AR's personnel performing similar functions. (3) CHR checks must be completed prior to accessing CHRI under the contract.	(1) Prior to performing work under the contract, obtain and submit relevant information of employees (and Sub-Contractors) requesting access to CHRI for CHR checks and wait for approval. (2) CHR checks must be completed prior to accessing CHRI under the contract.	(1) SCO/CA shall conduct CHR checks of Contractor personnel having access to CHRI, if authorized.	
6.02 - Requirements		(1) Ensure that each employee performing work under the contract is aware of the requirements of the OS and the state and federal laws governing the security and integrity of CHRI. (2) Confirm in writing that each employee has certified in writing that he/she understands the OS requirements and laws that apply to his/her responsibilities. (3) Maintain the employee certifications in a file that is subject to review during audits. (4) Employees shall make such certification prior to performing work under the contract.		

Responsibility Table for Non-Channeling

Outsource (OS) Section #	Authorized Recipient (AR)	Contractor	Chief Administrator (CA); CJIS Systems Agency (CSA)	United States Attorney General (US AG)
6.03 – Updated Personnel Records with Access to CHRI	Recommendation based on good business practice: (1) Maintain updated records of personnel who have access to CHRI, update those records within 24 hours when changes to that access occur. (2) If CHR check is required, maintain list of personnel who have successfully completed CHR checks.	(1) Maintain updated records of personnel who have access to CHRI, update those records within 24 hours when changes to that access occur. (2) If CHR check is required, maintain list of personnel who have successfully completed CHR checks. (3) Notify AR's within 24 hours when personnel additions or deletions occur.		
7.0 - System Security				
7.01 - CJIS Security Policy – See 2.02 - OS & CJIS Security Policy		(1) Ensure security system complies with <i>CJIS Security Policy</i> in effect at the time the OS is incorporated into the contract and with successor versions of the <i>CJIS Security Policy</i> .		
7.01(a) - Firewall	(1) Ensure encryption is used appropriately in accordance with the <i>CJIS Security Policy</i> .	(1) Implement a firewall-type device for all systems that can be accessed via WAN/LAN or Internet as specified in the <i>CJIS Security Policy</i> .		
7.01(b) - Encryption	(1) Ensure encryption is used appropriately in accordance with the <i>CJIS Security Policy</i> .	(1) Encrypt CHRI that is passed through a shared public carrier network.		
7.02 – CHRI and Media Storage and Disposal		(1) Provide for the secure storage & disposal of all hard copy and media associated with system to prevent access by unauthorized personnel. (a) Physically secure location. (b) Sanitize procedures for all fixed and non-fixed storage media. (c) Storage procedures for all fixed and non-fixed storage media.		
7.02(a) – CHRI Storage		(1) Store CHRI in a physically secure location.		
7.02(b) - Media Sanitization	(1) Ensure a procedure is in place for sanitizing all fixed storage media at completion of contract and/or before it is returned for maintenance, disposal, or re-use.	(1) Establish a procedure for sanitizing all fixed storage media at completion of contract and/or before it is returned for maintenance, disposal, or re-use.		

Responsibility Table for Non-Channeling

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	State Compact Officer (SCO); FBI Compact Officer (FBI CO); Chief Administrator (CA); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
		Sanitization procedures include overwriting the media and/or degaussing the media.		
7.02(c) – Disposal Procedure	(1) Ensure that a procedure is in place for the disposal and return of all non-fixed storage media.	(1) Establish a procedure for disposal and return of all non-fixed storage media.		
7.03 - Identification Requirement (See Section 11.08)	(1) Be assigned a unique identifying number by the Contractor.	(1) Identify each AR and sub-contractor by a unique identifying number.		
8.0 – Security Violations				
8.01 – Security Violation Policy (See Sections 2.07 & 3.03)	<p>(1) Develop & maintain a written policy for discipline of Contractor employees who violate the security provisions of the contract, including the OS.</p> <p>(2) Develop and maintain a written incident reporting plan for security events, to include violations and incidents.</p> <p>(3) Immediately (within four hours) notify SCO/CA and FBI CO of any security violation or termination of contract.</p> <p>(a) Provide written report of any security violation to the SCO/CA, if applicable, and the FBI CO, within 5 calendar days of receipt of written report from Contractor.</p> <p>(b) Written report must include corrective actions taken by Contractor and AR to resolve security violation.</p>	<p>(1) Pending investigation, upon detection or awareness, suspend any employee who commits a security violation from assignments with access to CHRI under the contract.</p> <p>(2) Immediately (within four hours) notify AR of any security violation or termination of the contract, to include unauthorized access to CHRI.</p> <p>(3) Within 5 calendar days of notification, provide AR written report documenting security violation, any corrective actions taken by Contractor, and the date, time, and summary of prior notification.</p>		
8.02 - Contract Termination (See Section 2.06)	<p>(1) Terminate the contract, when necessary, for security violations:</p> <p>(a) Involving CHRI obtained pursuant to the contract.</p> <p>(b) For the Contractor's failure to notify the AR of any security violation or to provide a written report concerning such violation.</p> <p>(c) If the Contractor refuses to or is incapable of taking corrective actions to successfully resolve a security violation.</p>			

Responsibility Table for Non-Channeling

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	State Compact Officer (SCO); FBI Compact Officer (FBI CO); Chief Administrator (CA); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
8.03(a) - CHRI Suspension or Termination (See Section 11.10 (a))			(1) If AR fails to provide a written report notifying the SCO/CA or the FBI CO of a security violation, or refuses to or is incapable of taking corrective action to successfully resolve a security violation, the CC or US AG may suspend or terminate the exchange of CHRI with AR pursuant to 28 CFR 906.2(d).	(1) If AR fails to provide a written report notifying the SCO/CA or the FBI CO of a security violation, or refuses to or is incapable of taking corrective action to successfully resolve a security violation, the CC or US AG may suspend or terminate the exchange of CHRI with AR pursuant to 28 CFR 906.2(d).
8.03(b) – Exchange of CHRI Reinstatement (See Section 11.10(b))	(1) If the exchange of CHRI is suspended, it may be reinstated after satisfactory written assurances have been provided by the SCO/CA, FBI CO, the AR and the Contractor to the CC Chairman or the US AG that the security violation has been resolved. (2) If the exchange of CHRI is terminated, inform the Contractor whether to delete or return records (including media) containing CHRI in accordance with the provisions and time frame specified.	(1) If the exchange of CHRI is suspended, it may be reinstated after satisfactory written assurances have been provided by the SCO/CA, FBI CO, the AR and the Contractor to the CC Chairman or the US AG that the security violation has been resolved. (2) If the exchange of CHRI is terminated, delete or return records (including media) containing CHRI, in accordance with the provisions and time frame as specified by AR.	(1) May reinstate after satisfactory written assurances have been provided to the CC Chair and US AG.	(1) If the exchange of CHRI is suspended, it may be reinstated after satisfactory written assurances have been provided by the SCO/CA, FBI CO, the AR, and the Contractor to the CC Chairman or the US AG that the security violation has been resolved.
8.04 - Security Violation Notification (See Section 11.11)	(1) Provide written notice (through SCO/CA if applicable) to FBI CO of the following: (a) Contract termination for security violations. (b) Security violations involving unauthorized access to CHRI. (c) Contractor's name and unique ID number, nature of security violation, whether violation was intentional, and number of times violation occurred.		(1) SCO/CA, if applicable, shall forward written notice to the FBI CO. (2) SCO/CA to ensure Contractor access to CHRI is terminated. (3) SCO/CA record date contract terminated and date Contractor access to CHRI is terminated.	
8.05 – Investigation Rights of Unauthorized Access to CHRI (See Section 11.12)			(1) SCO/CA reserves right to investigate or decline to investigate any report of unauthorized access to CHRI.	(1) CC and the US AG reserves right to investigate or decline to investigate any report of unauthorized access to CHRI.
8.06 - Audits			(1) SCO/CA reserve the right to audit AR and Contractor's operations and procedures at scheduled or unscheduled times. (2) State authorized to perform a final audit of the Contractor's systems after termination of contract.	(1) CC and US AG reserve the right to audit AR and Contractor's operations and procedures at scheduled or unscheduled times. (2) CC and US AG authorized to perform a final audit of Contractor systems after termination of contract.

Responsibility Table for Non-Channeling

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	State Compact Officer (SCO); FBI Compact Officer (FBI CO); Chief Administrator (CA); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
9.0 - Miscellaneous Provisions				
9.01 – OS	(1) This OS does not confer, grant, or authorize any rights, privileges, or obligations to any persons other than the Contractor, the AR, CO/CA (where applicable), and the FBI.	(1) This OS does not confer, grant, or authorize any rights, privileges, or obligations to any persons other than the Contractor, the AR, CO/CA (where applicable), and the FBI.	(1) This OS does not confer, grant, or authorize any rights, privileges, or obligations to any persons other than the Contractor, the AR, CO/CA (where applicable), and the FBI.	(1) This OS does not confer, grant, or authorize any rights, privileges, or obligations to any persons other than the Contractor, the AR, CO/CA (where applicable), and the FBI.
9.02 – CJIS Security Policy	(1) The <i>CJIS Security Policy</i> is incorporated by reference and made a part of this OS.	(1) The <i>CJIS Security Policy</i> is incorporated by reference and made a part of this OS.	(1) The <i>CJIS Security Policy</i> is incorporated by reference and made a part of this OS.	(1) The <i>CJIS Security Policy</i> is incorporated by reference and made a part of this OS.
9.03 & Footnote 5 – OS Stringency	(1) The CC, AR, and the CO/CA have the explicit authority to require more stringent standards than those contained in the OS.	(1) Comply with any additional conditions as required by the CC, AR, or the CO/CA.	(1) The CC, AR, and the CO/CA have the explicit authority to require more stringent standards than those contained in the OS.	(1) The CC, AR, and the CO/CA have the explicit authority to require more stringent standards than those contained in the OS.
9.04 – OS Modification	(1) The minimum security measures as outlined in this OS may only be modified by the CC. (2) Conformance to such security measures may not be less stringent than stated in this OS without the consent of the CC in consultation with the US AG.	(1) The minimum security measures as outlined in this OS may only be modified by the CC. (2) Conformance to such security measures may not be less stringent than stated in this OS without the consent of the CC in consultation with the US AG.	(1) The minimum security measures as outlined in this OS may only be modified by the CC. (2) Conformance to such security measures may not be less stringent than stated in this OS without the consent of the CC in consultation with the US AG.	(1) The minimum security measures as outlined in this OS may only be modified by the CC. (2) Conformance to such security measures may not be less stringent than stated in this OS without the consent of the CC in consultation with the US AG.
9.05 - OS Modification	(1) This OS may only be modified by the CC and may not be modified by the parties to the appended contract without the consent of the CC.	(1) This OS may only be modified by the CC and may not be modified by the parties to the appended contract without the consent of the CC.	(1) This OS may only be modified by the CC and may not be modified by the parties to the appended contract without the consent of the CC.	(1) This OS may only be modified by the CC and may not be modified by the parties to the appended contract without the consent of the CC.
9.06 - FBI CO Address	(1) Appropriate notices, assurances, and correspondence to the FBI CO, CC, and the US AG required by Section 8.0 of this OS shall be forwarded by First Class Mail to: FBI Compact Officer 1000 Custer Hollow Road Module D3 Clarksburg, WV 26306	(1) Appropriate notices, assurances, and correspondence to the FBI CO, CC, and the US AG required by Section 8.0 of this OS shall be forwarded by First Class Mail to: FBI Compact Officer 1000 Custer Hollow Road Module D3 Clarksburg, WV 26306	(1) Appropriate notices, assurances, and correspondence to the FBI CO, CC, and the US AG required by Section 8.0 of this OS shall be forwarded by First Class Mail to: FBI Compact Officer 1000 Custer Hollow Road Module D3 Clarksburg, WV 26306	(1) Appropriate notices, assurances, and correspondence to the FBI CO, CC, and the US AG required by Section 8.0 of this OS shall be forwarded by First Class Mail to: FBI Compact Officer 1000 Custer Hollow Road Module D3 Clarksburg, WV 26306

Responsibility Table for Non-Channeling

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	State Compact Officer (SCO); FBI Compact Officer (FBI CO); Chief Administrator (CA); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
10.0 – Exemption from Above Provisions				
10.01	<p>An IT contract need only include Sections 1.0, 2.01, 2.02, 2.03, 3.01, 6.0, 8.0, and 9.0 of this OS when all of the following conditions exist:</p> <p>(1) Access to CHRI by the IT contractor's personnel is limited solely for the development and/or maintenance of the AR's computer system;</p> <p>(2) Access to CHRI is incidental, but necessary, to the duties being performed by the IT contractor.</p> <p>(3) The computer system resides within the AR's facility:</p> <p>(4) The AR's personnel supervise or work directly with the IT contractor personnel;</p> <p>(5) The AR maintains complete, positive control of the IT contractor's access to the computer system and CHRI contained therein; and</p> <p>(6) The AR retains all the duties and responsibilities for the performance of its authorized NCJA functions, unless it executes a separate contract to perform such NCJA functions, subject to all applicable requirements, including the OS.</p>	<p>An IT contract need only include Sections 1.0, 2.01, 2.02, 2.03, 3.01, 6.0, 8.0, and 9.0 of this OS when all of the following conditions exist:</p> <p>(1) Access to CHRI by the IT contractor's personnel is limited solely for the development and/or maintenance of the AR's computer system;</p> <p>(2) Access to CHRI is incidental, but necessary, to the duties being performed by the IT contractor.</p> <p>(3) The computer system resides within the AR's facility:</p> <p>(4) The AR's personnel supervise or work directly with the IT contractor personnel;</p> <p>(5) The AR maintains complete, positive control of the IT contractor's access to the computer system and CHRI contained therein; and</p> <p>(6) The AR retains all the duties and responsibilities for the performance of its authorized NCJA functions, unless it executes a separate contract to perform such NCJA functions, subject to all applicable requirements, including the OS.</p>		
10.02 – Exemption	<p>An AR's contract where access to CHRI is limited solely for the purposes of the following:</p> <p>(a) storage (referred to as archiving in some states) of the CHRI at the Contractor's facility;</p> <p>(b) retrieval of the CHRI by Contractor personnel on behalf of the AR with appropriate security measures in place to protect the CHRI; and/or</p> <p>(c) destruction of the CHRI by Contractor personnel when not observed by the AR need</p>	<p>An AR's contract where access to CHRI is limited solely for the purposes of the following (a-c) need only include Sections 1.0, 2.01, 2.02, 2.03, 3.01, 4.0, 6.0, 8.0, and 9.0 of this OS when all of the following conditions exist (i-vii):</p> <p>(a) storage (referred to as archiving in some states) of the CHRI at the Contractor's facility;</p> <p>(b) retrieval of the CHRI by Contractor personnel on behalf of the AR with appropriate security measures in place to</p>		

Responsibility Table for Non-Channeling

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	State Compact Officer (SCO); FBI Compact Officer (FBI CO); Chief Administrator (CA); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
	<p>only include Sections 1.0, 2.01, 2.02, 2.03, 3.01, 4.0, 6.0, 8.0, and 9.0 of this OS when all of the following conditions exist:</p> <p>(i) Access to CHRI by the Contractor is limited solely for the purposes of:</p> <p>(i)(A) storage (referred to as archiving in some states) of the CHRI at the Contractor's facility;</p> <p>(i)(B) retrieval of the CHRI by Contractor personnel on behalf of the AR with appropriate security measures in place to protect the CHRI; and/or</p> <p>(i)(C) destruction of the CHRI by Contractor personnel when not observed by the AR;</p> <p>(ii) Access to CHRI is incidental, but necessary, to the duties being performed by the Contractor;</p> <p>(iii) The Contractor is not authorized to disseminate CHRI to any other agency or contractor on behalf of the AR;</p> <p>(iv) The Contractor's personnel are subject to the same CHR checks as the AR's personnel;</p> <p>(v) The CHR checks of the Contractor personnel are completed prior to work on the contract or agreement;</p> <p>(vi) The AR retains all other duties and responsibilities for the performance of its authorized NCJA functions, unless it executes a separate contract to perform such NCJA functions, subject to all applicable requirements, including the OS; and</p> <p>(vii) The Contractor stores the CHRI in a physically secure location.</p>	<p>protect the CHRI; and/or</p> <p>(c) destruction of the CHRI by Contractor personnel when not observed by the AR.</p> <p>(i) Access to CHRI by the Contractor is limited solely for the purposes of:</p> <p>(i)(A) storage (referred to as archiving in some states) of the CHRI at the Contractor's facility;</p> <p>(i)(B) retrieval of the CHRI by Contractor personnel on behalf of the AR with appropriate security measures in place to protect the CHRI; and/or</p> <p>(i)(C) destruction of the CHRI by Contractor personnel when not observed by the AR;</p> <p>(ii) Access to CHRI is incidental, but necessary, to the duties being performed by the Contractor;</p> <p>(iii) The Contractor is not authorized to disseminate CHRI to any other agency or contractor on behalf of the AR;</p> <p>(iv) The Contractor's personnel are subject to the same CHR checks as the AR's personnel;</p> <p>(v) The CHR checks of the Contractor personnel are completed prior to work on the contract or agreement;</p> <p>(vi) The AR retains all other duties and responsibilities for the performance of its authorized NCJA functions, unless it executes a separate contract to perform such NCJA functions, subject to all applicable requirements, including the OS; and</p> <p>(vii) The Contractor stores the CHRI in a physically secure location.</p>		
Section 11.0 – Duties of the SCO/CA				

Responsibility Table for Non-Channeling

Outsourcing (OS) Section #	Authorized Recipient (AR)	Contractor	Chief Administrator (CA); CJIS Systems Agency (CSA)	United States Attorney General (US AG)
11.01 – Outsourcing Request (See Section 2.01)			(1) Review legal authority and respond in writing to the AR's request to outsource noncriminal justice administrative functions.	
11.02 – Access to Contract (See Section 2.03(d))			(1) Reserves the right to review relevant portions of the outsourcing contract relating to CHRI throughout the duration of the contract approval.	
11.03 – Criminal History Record (CHR) Checks (See Section 2.03(a), 6.01 and Footnote 4)			(1) Ensure criminal history record checks on approved Contractor and Sub-Contractor employees with access to CHRI are completed by the AR, if such checks are required or authorized of the AR personnel by federal statute, or executive order, or state statute approved by the U.S. AG under Pub. L. 92-544. Criminal history record checks should be no less stringent than the checks performed on the AR personnel. Criminal history record checks must be completed prior to access CHRI under the contract.	
11.04 – Records and Topological Drawing (See Section 2.04)			(1) Coordinate with the AR for the review and approval of the Contractor's Topological drawing which depicts the interconnectivity of the Contractor's network configuration as it relates to the outsourcing function(s).	
11.05 – 90 Day Compliance Review (See Section 2.05)			<p>(1) Work in coordination with the AR to conduct an audit of the Contractor within 90 days of the date the Contractor first receives CHRI under the approved outsourcing agreement.</p> <p>(2) Review the AR's audit certification to ensure compliance with the OS.</p> <p>(i) Address concerns with the AR resulting in non-compliance with the 90 day audit of the Contractor.</p> <p>(ii) Have the right to terminate an AR's outsourcing approval to a Contractor(s) for failure or refusal to correct a non-compliance issue(s).</p>	

Outsourcing (OS)	Responsibility Table for Non-Channeling				State Security Council (CJIS); Security Council (CC); Attorney General (S AG)
11.06 – Security Program Review (See Section 3.06)			(1) Coordinate with the AR to review the Contractor's Security Program. (2) The program shall describe the implementation of the security requirements outlined in the OS and the <i>CJIS Security Policy</i> . (3) During the review, provisions will be made to update the Security Program to address security events and to ensure changes in policies and standards, as well as changes in federal and state law, are incorporated.		
11.07 – Security Inspection (See Section 3.05)			(1) Audit the AR and/or Contractor's operations and procedures. This may be done at scheduled and unscheduled times.		
11.08 – Identification Requirement (See Section 7.03)			(1) Assign a unique identifying number to each AR, Contractor, or sub-Contractor to ensure system security.		
11.09 – Security Violation Policy (See Section 8.01)			(1) Require immediate (within four hours) notification by the AR of any security event, to include unauthorized access to CHRI made available pursuant to the contract. (2) Receive a written report from the AR of any security event (to include unauthorized access to CHRI by the Contractor) within five calendar days of receipt of the written report from the Contractor, that must include any corrective actions taken by the Contractor and AR to resolve such security event.		
11.10 (a) – CHRI Suspension or Termination (See Section 8.03(a))			Suspension or termination of the exchange of CHRI for security events. (1) May suspend or terminate the exchange of CHRI for security events or refusal or incapability to take corrective action to successfully resolve a security event.		
11.10 (b) – Exchange of CHRI Reinstatement (See Section 8.03(b))			(1) May reinstate access to CHRI between the AR and the Contractor after receiving the written assurance(s) of corrective action(s) from the AR and/or the Contractor.		

Responsibility Table for Non-Channeling				
Outsource (OS) S				in (CJIS); cil (CC); ttorney AG)
11.11 – Security Violation Notification (See Section 8.04)			<p>(1) Provide written notification to the FBI CO of the termination of a contract for security events to include:</p> <p>(a) the security events involving access to CHRI</p> <p>(b) the Contractor’s name and unique identification number</p> <p>(c) the nature of the security event;</p> <p>(d) whether the event was intentional</p> <p>(e) and the number of times the event occurred.</p>	
11.12 – Investigation Rights of Unauthorized Access to CHRI (See Section 8.05)			<p>(1) Reserves the right to investigate or decline to investigate any report of unauthorized access to CHRI.</p>	
11.13 – Audits (See Section 8.06)			<p>(1) Is Authorized to perform a final audit of the Contractor’s system following termination of contract.</p>	

Responsibility Table for Channeling

Security and Management Control Outsourcing Standard (OS) for Channelers

OS dated 11/06/2014, table updated 12/17/2014

Outsourcing Standard (OS) Section #	Authorized Recipient (AR) State Identification Bureau on behalf of the Local/State Agency	Contractor	State Compact Officer (SCO); Chief Administrator (CA); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); FBI Compact Officer (FBI CO); Compact Council (CC); United States Attorney General (US AG)
Section 2.0 - Responsibilities of the AR				
2.01 - Outsourcing Request Footnote 2 - Audit Requirements Footnote 3 - Outsourcing Approval	AR shall: (1) Request and receive written permission from the FBI CO. (2) Provide FBI CO copies of the specific authority for the outsourced work, criminal history record check requirements, and/or a copy of relevant portions of the contract as requested. (3) Conduct audits of Contractor, as necessary. (4) Review audit reports and impose sanctions as necessary.			FBI CO shall: (1) approve/disapprove request in writing. (2) FBI CO may not grant such permission unless he/she has implemented a federal audit program to, at a minimum, triennially audit a representative sample of the Contractors and ARs engaging in outsourcing with the first of such audits to be conducted within one year of the date the Contractor first receives CHRI under the approved outsourcing agreement. (3) FBI CO will review copies of the specific authority for the outsourced work, criminal history record check requirements, and/or a copy of relevant portions of the contract if requested. CJIS Audit Unit shall: (1) Conduct required audits of AR and Contractor and audit on behalf of the CC. (2) CJIS/CC to review audit reports and impose sanctions as necessary.
2.02 - Contract 2.03(c) & 7.01 & 9.02 – OS and CJIS Security Policy	(1) Execute contract or agreement prior to providing a Contractor access to CHRI. (2) Ensure that the most updated versions of both the OS and/or the <i>CJIS Security Policy</i> are incorporated by reference at the time of the contract, contract renewal, or within 60 calendar days of the notification period, whichever is sooner.	(1) Ensure that the most current versions of both the OS and the <i>CJIS Security Policy</i> are incorporated by reference and appended to the contract at the time of the initial contract, contract renewal, and/or Option renewal.		(1) FBI CO shall make available the most current version of both the OS and the <i>CJIS Security Policy</i> to the AR within 60 calendar days (unless otherwise directed) of notification of successor versions. (2) Within 60 calendar days of changes and updates to the OS and the CJIS Security Policy, CJIS shall notify Contractors of such changes or updates.
2.03 - Access to CHRI	When Contractor will have access to CHRI, the AR shall: (1) Specify terms and conditions of access.			(1) CJIS Audit Unit shall conduct 90-day, one year, and triennial audits of Contractors.

Responsibility Table for Channeling

Outsourcing Standard (OS) Section #	Authorized Recipient (AR) State Identification Bureau on behalf of the Local/State Agency	Contractor	State Compact Officer (SCO); Chief Administrator (CA); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); FBI Compact Officer (FBI CO); Compact Council (CC); United States Attorney General (US AG)
	<p>(2) Limit the use of the information to the purposes for which provided.</p> <p>(3) Prohibit dissemination except as authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the CC and the US AG.</p> <p>(4) Ensure security and confidentiality of the information to include confirmation that the intended recipient is authorized to receive CHRI.</p> <p>(5) Provide for audits and sanctions.</p> <p>(6) Provide conditions for termination of the contract.</p> <p>(7) Ensure Contractor personnel comply with OS.</p> <p>(8) May conduct 90-day, one year, and triennial audits of Contractors.</p>			
2.03(a) – Criminal History Record (CHR) Checks	<p>Recommendation based on good business practice:</p> <p>(1) Maintain updated records of personnel who have access to CHRI, update those records within 24 hours when changes to that access occur.</p>	<p>(1) Provide personnel information relevant for a CHR check.</p> <p>(2) Provide updates of personnel changes to CJIS within 24 hours of changes.</p>		<p>(1) CJIS shall conduct CHR checks of Contractor personnel having access to CHRI.</p> <p>(2) CJIS shall maintain updated records of Contractor personnel who have access to CHRI and update those records within 24 hours when changes to that access occur.</p> <p>(3) CJIS shall maintain list of Contractor personnel who have successfully completed CHR checks.</p>
2.03(b) - Site Security	(1) May ensure that a Contractor maintains site(s) security.	(1) Maintain site(s) security.		(1) FBI shall ensure that Contractor maintain site(s) security.
2.03(c) - OS and CJIS Security Policy	See 2.02			See 2.02
2.03(d) & 3.02 - Security Program	<p>AR may:</p> <p>(1) Ensure that the Contractor establishes and administers an IT Security Program.</p> <p>(2) Provide written approval of a Contractor's Security Program. However, this</p>	<p>Contractor shall:</p> <p>(1) Develop, document, administer, and maintain a Security Program (Physical, Personnel, and IT) to comply with the most current OS and most</p>		<p>FBI shall:</p> <p>(1) Ensure that the Contractor establishes and administers a Security Program.</p> <p>(2) Provide the written approval of a Contractor's Security Program.</p>

Responsibility Table for Channeling

Outsourcing Standard (OS) Section #	Authorized Recipient (AR) State Identification Bureau on behalf of the Local/State Agency	Contractor	State Compact Officer (SCO); Chief Administrator (CA); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); FBI Compact Officer (FBI CO); Compact Council (CC); United States Attorney General (US AG)
	approval is not in lieu of the FBI's written approval.	current <i>CJIS Security Policy</i> . (2) Provide written security program to FBI for approval and if requested to the AR. (3) Security Program shall describe the implementation of the security requirements described in this OS and the <i>CJIS Security Policy</i> . (4) Set, maintain, and enforce the standards for selection, supervision, and separation of personnel who have access to CHRI.		
2.03(e) - Penetration Testing	(1) Shall allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system.			(1) CJIS may test ability to penetrate network through the external network connection or system.
2.03(f) - Access to Contract	(1) Make available to the FBI CO the relevant portions of the current and approved contract relating to CHRI, upon request.	(1) Make available to the FBI CO the relevant portions of the current and approved contract relating to CHRI, upon request.		(1) CJIS may request relevant portions of the current and approved contract relating to CHRI.
2.04 - Records and Topological Drawing	(1) Understand the communications and record capabilities of the Contractor which has access to federal or state records through, or because of, its outsourcing relationship with the AR. (2) May maintain an updated topological drawing which depicts the interconnectivity of the Contractor's network configuration.	(1) Provide updated topological drawings depicting the interconnectivity of the network configuration to the FBI and, if requested, to the AR.		(1) FBI shall maintain an updated topological drawing which depicts the interconnectivity of the Contractor's network configuration.
2.05 - 90 Day Compliance Review	(1) Responsible for the actions of Contractor and monitoring the Contractor's compliance to the terms and conditions of the OS.			(1) CJIS Audit Unit shall certify to the FBI CO that an audit was conducted with the Contractor within 90 days of the date the Contractor first receives CHRI under the approved outsourcing agreement.
2.06 - Contract Termination	(1) Provide written notice of any early voluntary termination of the contract to the FBI CO.			
2.07 - ISO Appointment	(1) Appoint an Information Security Officer (ISO) to: (a) Serve as the security POC for the FBI CJIS Division ISO;			

Responsibility Table for Channeling

Outsourcing Contract # (OS) Section #	State Identification Bureau on behalf of the Local/State Agency	Contractor	Chief Administrator (CA); CJIS Systems Agency (CSA)	n (CJIS); er (FBI CO); Compact Council (CC); United States Attorney General (US AG)
	<p>(b) Document technical compliance with the OS; and</p> <p>(c) Establish a security incident response and reporting procedure to discover, investigate, document, and report on major incidents that significantly endanger the security or integrity of the NCJ agency systems to the state's CJIS Systems Officer and the FBI CJIS Division ISO.</p>			
3.0 - Responsibilities of the Contractor				
3.01 - Regulation Compliance		<p>(1) Contractor and its employees shall comply with all federal and state laws, regulations, and standards (including the <i>CJIS Security Policy</i>) as well as with rules, procedures, and standards established by the CC and the US AG.</p>		
3.02 - Security Program – See 2.03(d)	See 2.03(d)			See 2.03(d)
3.03 - Security Requirements		<p>(1) Requirements for a Security Program <u>should include</u>, at a minimum:</p> <p>(a) Description of the implementation of the security requirements described in the OS and the <i>CJIS Security Policy</i>.</p> <p>(b) Security training.</p> <p>(c) Guidelines for documentation of security violations.</p> <p>(d) Standards for the selection, supervision, and separation of personnel with access to CHRI.</p> <p>*If using a corporate policy, it must meet the requirements outlined in the OS and the <i>CJIS Security Policy</i>. If the corporate policy is not this specific, it must flow down to a level where the documentation supports these requirements.</p>		
3.04 – Security Program Management		<u>Shall be:</u>		

Responsibility Table for Channeling

Outsourcing (OS) Contractor	On behalf of the Local/State Agency	Contractor	CJIS Systems Agency (CSA)	on (CJIS); er (FBI CO); cil (CC); United States Attorney General (US AG)
		<p>(1) Accountable for the management of the Security Program.</p> <p>(2) Responsible for reporting all security violations of the OS to the AR.</p>		
3.05 - Security Training Program	<p>If training requirement retained by AR:</p> <p>(1) Develop a Security Training Program for all Contractor personnel with access to CHRI prior to their appointment/assignment.</p> <p>(2) Provide training upon receipt of notice from the FBI CO on any changes to federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the CC and the US AG.</p> <p>(3) Provide annual refresher training, not later than the anniversary date of the contract, and may certify in writing to the FBI that annual refresher training was completed for those Contractor personnel with access to CHRI.</p>	<p>(1) Except when the training requirement is retained by the AR, the Contractor shall develop a Security Training Program for all Contractor personnel with access to CHRI prior to their appointment/assignment.</p> <p>(2) Provide training upon receipt of notice from the FBI CO or SCO/CA on any changes to federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the CC and the US AG.</p> <p>(3) Provide annual refresher training, not later than the anniversary date of the contract, and certify in writing to the FBI that annual refresher training was completed for those Contractor personnel with access to CHRI.</p>		<p>FBI shall:</p> <p>(1) Review and provide to a Contractor written approval/disapproval of the Contractor's Security Training Program (unless retained by the AR).</p> <p>(2) Ensure that annual refresher training was completed by those Contractor personnel with access to CHRI.</p>
3.06 - Security Inspection	(1) May perform announced and unannounced audits and security inspections.	(1) Make its facilities available for announced and unannounced audits and security inspections performed by the AR or the FBI on behalf of the CC.		(1) FBI , on behalf of CC, shall perform announced and unannounced audits and security inspections.
3.07 - Security Program Review (See Sectin 3.02)	<p>(1) May review Contractor's Security Program.</p> <p>(2) During this review, provision will be made to update the Security Program to address security violations and to ensure changes in policies and standards as well as changes in federal and state law are incorporated.</p>			<p>(1) CJIS shall review Contractor's Security Program.</p> <p>(2) During this review, provision will be made to update the Security Program to address security violations and to ensure changes in policies and standards as well as changes in federal and state law are incorporated.</p>
3.08 - Maintenance of CHRI	(1) Manner of and time frame for CHRI dissemination by the Contractor shall be specified in the contract or agreement.	<p>(1) Maintain CHRI only for period of time necessary to fulfill its contractual obligations.</p> <p>(2) CHRI disseminated by a Contractor to an AR via an authorized Web site</p>		

Responsibility Table for Channeling				
Outsource (OS)	Department of the Army, State Agency		CJIS Systems Agency (CSA)	Department of Justice (DOJ) Federal Bureau of Investigation (FBI CO); Attorney General (AG); Department of Justice (DOJ) Attorney General (US AG)
		shall remain on such Web site only for the time necessary to meet the AR's requirements but in no event shall that time exceed 30 calendar days. (3) Destroy CHRI immediately after confirmation of successful receipt by the AR. (4) Manner of and time frame for CHRI dissemination to an AR shall be specified in the contract or agreement.		
3.09 - CHRI Logging		(1) Maintain log of any CHRI dissemination for a minimum of 365 days.		
3.10 - Access to Contract	See 2.03(f)	See 2.03(f)		See 2.03(f)
4.0 - Site Security				
4.01 - Physically Secure Location		(1) Maintain a physically secure site(s).		<u>FBI shall:</u> (1) Ensure that a Contractor's site is a physically secure location to protect against any unauthorized access to CHRI.
4.02 - Visitor Escort		(1) Only authorized personnel shall escort all visitors to computer centers and/or terminal areas.		
4.03 - Contractor with Direct Access		(1) Any Contractor with direct access to CHRI shall allow the FBI to conduct periodic penetration testing.		(1) <u>FBI</u> may conduct periodic penetration testing.
5.0 - Dissemination				
5.01 - System Access	(1) Ensure that access to the system is provided to employees of the Contractor, employees of the AR, and such other persons as authorized by the AR for official purposes consistent with the appended contract.	(1) Ensure that access to the system is provided to employees of the Contractor, employees of the AR, and such other persons as authorized by the AR for official purposes consistent with the appended contract.		(1) <u>CJIS</u> will ensure that access to the system is provided to employees of the Contractor, employees of the AR, and such other persons as authorized by the AR for official purposes consistent with the appended contract.
5.02 - Official Use of CHRI	(1) Ensure access to the system is available only for official purposes consistent with the appended contract. (2) Ensure any dissemination of CHRI data to authorized	(1) Ensure access to the system is available only for official purposes consistent with the appended contract. (2) Ensure any dissemination of CHRI		<u>CJIS</u> will: (1) Ensure access to the system is available only for official purposes consistent with the appended contract.

Outsourcing (OS)	Responsibility Table for Channeling				FBI CJIS Division (CJIS); Department of Justice (DOJ); Federal Bureau of Investigation (FBI CO); Attorney General (CC); Attorney General (US AG)
					General (US AG)
	employees of the Contractor is to be for official purposes only.	data to authorized employees of the Contractor is to be for official purposes only.			(2) Ensure any dissemination of CHRI data to authorized employees of the Contractor is to be for official purposes only.
5.03 - CHRI Dissemination	(1) Ensure information contained in or about the system will not be provided to agencies other than the AR or another entity which is specifically designated in the contract.	(1) Ensure information contained in or about the system will not be provided to agencies other than the AR or another entity which is specifically designated in the contract.			(1) CJIS will ensure information contained in or about the system will not be provided to agencies other than the AR or another entity which is specifically designated in the contract.
5.04 - Dissemination Authority	(1) Authorize any dissemination by the Contractor of CHRI that are within the guidelines of federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the CC and the US AG.	(1) Not disseminate CHRI without the consent of the AR, and as specifically authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the CC and the US AG.			(1) CJIS will ensure that the Contractor does not disseminate CHRI without the consent of the AR, and as specifically authorized by federal laws, regulations, and standards established by the CC and the US AG.
5.05 – Dissemination Log		(1) Maintain an up-to-date log of CHRI for a minimum one year retention period that must clearly identify: (a) AR and the secondary recipient with unique identifiers, (b) Record disseminated, (c) Date of dissemination, (d) Statutory authority for dissemination, and (e) Means of dissemination			(1) CJIS will ensure that the Contractor will maintain an up-to-date log of CHRI for a minimum one year retention period that must clearly identify: (a) AR and the secondary recipient with unique identifiers, (b) Record disseminated, (c) Date of dissemination, (d) Statutory authority for dissemination, and (e) Means of dissemination
5.06 – Unauthorized Access		(1) If CHRI is stored or disseminated in an electronic format, protect against unauthorized access to the equipment and any of the data. (2) In no event shall responses containing CHRI be disseminated other than as governed by this OS or more stringent contract requirements.			CJIS will: (1) Protect against unauthorized access to the equipment and any of the data if CHRI is stored or disseminated in an electronic format.
5.07 - Access Attempts		(1) Shall not attempt access for inappropriate or illegal activities. (2) Record and review access attempts to detect inappropriate or illegal activity.			(1) CJIS may record and review access attempts for detection of inappropriate or illegal activities.

Outsourcing (OS) S	Authorized Personnel (AP)	State Contract Officer (SCO)	FBI CJIS Division (CJIS); FBI Contract Officer (FBI CO); FBI Criminal Justice Institute (CJ); FBI Attorney General (AG)	
			Responsibility Table for Channeling	
5.08 - Contingency Plan		(1) Establish a documented contingency plan as defined in the <i>CJIS Security Policy</i> and approved by the FBI.		(1) FBI shall approve a Contractor's documented contingency plan as defined in the <i>CJIS Security Policy</i> .
6.0 - Personnel Security				
6.01 - Personnel CHR Check		(1) Prior to performing work under the contract, obtain and submit relevant information of Contractor (and approved Sub-Contractor) personnel requesting access to CHRI for CHR checks and wait for approval.		(1) The FBI shall process CHR checks on Contractor (and approved Sub-Contractor) personnel having access to CHRI. CHR checks must be completed prior to accessing CHRI under the contract. (2) The FBI shall notify Contractor of CHR check decision.
6.02 - Requirements		(1) Shall ensure that each employee performing work under the contract is aware of the requirements of the OS and the state and federal laws governing the security and integrity of CHRI. (2) Shall confirm in writing that each employee has certified in writing that he/she understands the OS requirements and laws that apply to his/her responsibilities. (3) Shall maintain the employee certifications in a file that is subject to review during audits. (4) Employees shall make such certification prior to performing work under the contract.		(1) The CJIS Audit Unit shall review confirmation certifications during audits.
6.03 - Updated Personnel Records with Access to CHRI	(1) May request and maintain updated records of personnel with access to CHRI.	(1) Shall maintain updated records of personnel who have access to CHRI, update those records within 24 hours when changes to that access occur, and maintain a list of personnel who have successfully completed CHR checks. (2) Shall notify FBI within 24 hours when additions or deletions occur.		(1) CJIS shall maintain list of personnel who successfully complete the CHR check. (2) CJIS shall update the list of Contractor personnel when additions or deletions occur.
7.0 - System Security				

Outsourcing Standard (OS) Section #	Authorized Recipient (AR) State Identification Bureau on behalf of the Local/State Agency	Contractor	State Compact Officer (SCO); Chief Administrator (CA); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); FBI Compact Officer (FBI CO); Compact Council (CC); United States Attorney General (US AG)
Responsibility Table for Channeling				
7.01 - CJIS Policy - Security Policy		the OS is incorporated into the contract and with successor versions of the <i>CJIS Security Policy</i> .		
7.01(a) - Firewall		<p>(1) Protect the CHRI with firewall-type devices to prevent such unauthorized access if CHRI can be accessed by unauthorized personnel via WAN/LAN or the Internet.</p> <p>(2) Implement a minimum firewall profile as specified by the <i>CJIS Security Policy</i> in order to provide a point of defense and a controlled and audited access to CHRI, both from inside and outside the networks.</p>		(1) CJIS will ensure firewall-type devices are implemented to ensure unauthorized access to CHRI as specified in the <i>CJIS Security Policy</i> .
7.01(b) - Encryption		(1) Encrypt CHRI that is passed through a shared public carrier network.		
7.02 - CHRI and Media Storage and Disposal		(1) Provide for the secure storage & disposal of all hard copy and media associated with system.		
7.02(a) - CHRI Storage		(1) Store CHRI in a physically secure location.		
7.02(b) - Media Sanitization	(1) Ensure a procedure is in place for sanitizing all fixed storage media (e.g., disks, drives, backup storage) at the completion of the contract and/or before it is returned for maintenance, disposal, or reuse.	(1) Establish a procedure for sanitizing all fixed storage media at completion of contract and/or before it is returned for maintenance, disposal, or re-use. Sanitization procedures include overwriting the media and/or degaussing the media.		
7.02(c) - Disposal Procedure	(1) Ensure a procedure is in place for the disposal or return of all non-fixed storage media (e.g., hard copies, print-outs).	(1) Establish a procedure for disposal and return of all non-fixed storage media.		
7.03 - Identification Requirement	(1) Be assigned a unique identifying number by CJIS or the Contractor.	(1) Identify each AR and Sub-Contractor by a unique identifying number.		<p>(1) CJIS shall assign a unique identifier to each Contractor.</p> <p>(2) CJIS may assign a unique identifying number to the AR.</p>
8.0 - Security Violations				
8.01 - Security Violation Policy	(1) Immediately (within four hours) notify FBI CO of any security violation or termination of contract.	(1) Develop & maintain a written policy for discipline of employees who violate security		

Outsourcing Standard (OS) Section #	Authorized Recipient (AR) State Identification Bureau on behalf of the Local/State Agency	Contractor	State Compact Officer (SCO); Chief Administrator (CA); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); FBI Compact Officer (FBI CO); Compact Council (CC); United States Attorney General (US AG)
	(2) Provide written report of	provisions of the contract.		
<h2>Responsibility Table for Channeling</h2>				
	<p>from Contractor.</p> <p>(3) Written Report must include corrective actions taken by Contractor and AR to resolve security violation.</p>	<p>employee who commits a security violation from assignments in which he/she has access to CHRI, pending investigation.</p> <p>(3) Immediately (within four hours) notify AR and the FBI of any security violation to include unauthorized access to CHRI.</p> <p>(4) Within 5 calendar days of notification, provide AR and the FBI a written report documenting security violation, any corrective actions taken by Contractor, and the date, time, and summary of prior notification.</p>		
8.02 - Contract Termination	<p>(1) Terminate Contract, when necessary, for security violations:</p> <p>(a) Involving CHRI obtained pursuant to the contract.</p> <p>(b) For the Contractor's failure to notify the AR of any security violation or to provide a written report concerning such violation.</p> <p>(c) If the Contractor refuses to or is incapable of taking corrective actions to successfully resolve a security violation.</p>			
8.03(a) - CHRI Suspension or Termination				<p>(1) If AR fails to provide a written report notifying the FBI CO of a security violation, or refuses to or is incapable of taking corrective action to successfully resolve a security violation, the CC or US AG may suspend or terminate the exchange of CHRI with AR pursuant to 28 CFR 906.2(d).</p>
8.03(b) - Exchange of CHRI Reinstatement	<p>(1) The AR and Contractor shall provide to the CC Chairman or the US AG satisfactory written assurances that the security violation has been resolved.</p> <p>(2) If the exchange of CHRI is terminated, inform the</p>	<p>(1) The AR and Contractor shall provide to the CC Chairman or the US AG satisfactory written assurances that the security violation has been resolved.</p>		<p>(1) If the exchange of CHRI is suspended, it may be reinstated after satisfactory written assurances have been provided to the CC Chairman or the US AG, by the AR and the Contractor that the security violation has been resolved.</p>

Outsourcing Standard (OS) Section #	Authorized Recipient (AR) State Identification Bureau on behalf of the Local/State Agency	Contractor	State Compact Officer (SCO); Chief Administrator (CA); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); FBI Compact Officer (FBI CO); Compact Council (CC); United States Attorney General (US AG)
	Contractor whether to delete or return records (including media) containing CHRI is	(2) If the exchange of CHRI is terminated, delete or return records (including media) containing CHRI is		
Responsibility Table for Channeling				
		as specified by AR.		
8.04 - Security Violation Notification	<p>(1) Provide written notice to the FBI CO of the following:</p> <p>(a) Contract termination for security violations.</p> <p>(b) Security violations involving unauthorized access to CHRI.</p> <p>(c) Contractor's name and unique ID number, nature of security violation, whether violation was intentional, and number of times violation occurred.</p>			
8.05 - Investigation Rights of Unauthorized Access to CHRI			(1) SCO/CA, CC and the US AG reserves right to investigate or decline to investigate any report of unauthorized access to CHRI.	(1) SCO/CA, <u>CC</u> and the <u>US AG</u> reserves right to investigate or decline to investigate any report of unauthorized access to CHRI.
8.06 - Audits			<p>(1) SCO/CA, CC and US AG reserve the right to audit AR and Contractor's operations and procedures at scheduled or unscheduled times.</p> <p>(2) CC, US AG, and the state are authorized to perform a final audit of Contractor systems after termination of contract.</p>	<p>(1) SCO/CA, <u>CC</u> and <u>US AG</u> reserve the right to audit AR and Contractor's operations and procedures at scheduled or unscheduled times.</p> <p>(2) <u>CC</u>, <u>US AG</u>, and the state are authorized to perform a final audit of Contractor systems after termination of contract.</p>
9.0 - Miscellaneous Provisions				
9.01 - OS	(1) This OS does not confer, grant, or authorize any rights, privileges, or obligations to any persons other than the Contractor, the AR, SCO/CA (where applicable), CJIS Systems Agency and the FBI.	(1) This OS does not confer, grant, or authorize any rights, privileges, or obligations to any persons other than the Contractor, the AR, SCO/CA (where applicable), CJIS Systems Agency and the FBI.	(1) This OS does not confer, grant, or authorize any rights, privileges, or obligations to any persons other than the Contractor, the AR, SCO/CA (where applicable), CJIS Systems Agency and the FBI.	(1) This OS does not confer, grant, or authorize any rights, privileges, or obligations to any persons other than the Contractor, the AR, SCO/CA (where applicable), CJIS Systems Agency and the FBI.
9.02 - CJIS Security Policy	(1) The CJIS Security Policy is incorporated by reference and made a part of this OS.	(1) The CJIS Security Policy is incorporated by reference and made a part of this OS.	(1) The CJIS Security Policy is incorporated by reference and made a part of this OS.	(1) The CJIS Security Policy is incorporated by reference and made a part of this OS.
9.03 & footnote 4 - OS Stringency	(1) The CC, AR, and the SCO/CA have the explicit authority to require more stringent standards than those contained in the OS.	(1) Comply with any additional conditions as required by the CC, AR, or the SCO/CA.	(1) The CC, AR, and the SCO/CA have the explicit authority to require more stringent standards than those contained in the OS.	(1) The <u>CC</u> , AR, and the SCO/CA have the explicit authority to require more stringent standards than those contained in the OS.

Outsourcing Standard (OS) Section #	Authorized Recipient (AR) State Identification Bureau on behalf of the Local/State Agency	Contractor	State Compact Officer (SCO); Chief Administrator (CA); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); FBI Compact Officer (FBI CO); Compact Council (CC); United States Attorney General (US AG)
9.04 - OS Modification	(1) The minimum security measures as outlined in this OS may only be modified by	(1) The minimum security measures as outlined in this OS may only be	(1) The minimum security measures as outlined in this OS may only be modified by the CC.	(1) The minimum security measures as outlined in this OS may only be modified by the CC.
<div>Responsibility Table for Channeling</div>				
	less stringent than stated in this OS without the consent of the CC in consultation with the US AG.	be less stringent than stated in this OS without the consent of the CC in consultation with the US AG.	OS without the consent of the CC in consultation with the US AG.	OS without the consent of the CC in consultation with the US AG.
9.05 - OS Modification	(1) This OS may only be modified by the CC and may not be modified by the parties to the appended contract without the consent of the CC.	(1) This OS may only be modified by the CC and may not be modified by the parties to the appended contract without the consent of the CC.	(1) This OS may only be modified by the CC and may not be modified by the parties to the appended contract without the consent of the CC.	(1) This OS may only be modified by the CC and may not be modified by the parties to the appended contract without the consent of the CC.
9.06 - FBI CO Address	(1) Appropriate notices, assurances, and correspondence to the FBI CO, CC, and the US AG required by Section 8.0 of this OS shall be forwarded by First Class Mail to: FBI Compact Officer 1000 Custer Hollow Road Module D-3 Clarksburg, WV 26306	(1) Appropriate notices, assurances, and correspondence to the FBI CO, CC, and the US AG required by Section 8.0 of this OS shall be forwarded by First Class Mail to: FBI Compact Officer 1000 Custer Hollow Road Module D-3 Clarksburg, WV 26306	(1) Appropriate notices, assurances, and correspondence to the FBI CO, CC, and the US AG required by Section 8.0 of this OS shall be forwarded by First Class Mail to: FBI Compact Officer 1000 Custer Hollow Road Module D-3 Clarksburg, WV 26306	(1) Appropriate notices, assurances, and correspondence to the FBI CO, CC, and the US AG required by Section 8.0 of this OS shall be forwarded by First Class Mail to: FBI Compact Officer 1000 Custer Hollow Road Module D-3 Clarksburg, WV 26306

Authorized Recipient's Responsibilities

Prior to engaging in the outsourcing of any noncriminal justice administrative functions, the AR is required to request and receive written permission from the SCO/CA (non-channeling) or the FBI Compact Officer (channeling). The following sections provide examples of Non-Channeling and Channeling documentation and may be used as a reference when drafting documents relating to the outsourcing of noncriminal justice administrative functions.

Non-Channeling Sample Documentation

- Sample Authorized Recipient Request Letter for Non-Channeling
- Sample Language between the Authorized Recipient and Contractor regarding Noncriminal Justice Outsourcing Functions for Non-Channeling

Channeling Sample Documentation

- Sample Authorized Recipient Request Letter to Use a Channeler
- Sample FBI Response Letter for Channeler Request
- Sample Language between the Authorized Recipient and Channeler regarding Noncriminal Justice Outsourcing Functions for Channeling

Examples of Non-Channeling Documentation

Sample Authorized Recipient Request Letter for Non-Channeling

REQUEST LETTER
FOR **[insert Authorized Recipient's name]** TO USE
[insert Contractor's name] AS A CONTRACTOR
FOR NONCRIMINAL JUSTICE ADMINISTRATIVE FUNCTIONS

[State Compact Officer/Chief Administrator's name]
[State Agency]
[Address]
[City, State Zip Code]

Dear **[insert State Compact Officer/Chief Administrator's name]**:

[Insert Authorized Recipient's name], the Authorized Recipient, requests permission to use **[insert Contractor's name]** as a contractor to outsource noncriminal justice administrative functions relating to the processing of criminal history record information (CHRI) on our behalf. This would include **[insert all functions that may apply. For example, obtaining missing dispositions, making determinations and recommendations, off-site storage of criminal history record information and its corresponding fingerprint submissions, etc.]** **[Insert Authorized Recipient's name]** and **[insert Contractor's name]** have entered into an agreement in which **[insert Contractor's name]** will act on our behalf in accordance with the Security and Management Control Outsourcing Standard (Outsourcing Standard) for Non-Channelers. **[Insert Authorized Recipient's name]** is authorized to perform background checks pursuant to the **[insert the legal citation of the statute or public law that requires or authorizes the Authorized Recipient to have access to CHRI.]**

Upon execution of the Contract, **[insert Authorized Recipient's name]** will take responsibility for **[insert Contractor's name]** compliance with the terms of the Contract, to include the Outsourcing Standard for Non-Channelers, and will notify the FBI Compact Officer of any violations.

Sincerely,

[insert name]
[insert title]
[insert address]
[insert phone number]
[insert email address]
[insert fax number]

Sample Language between the Authorized Recipient and Contractor regarding Noncriminal Justice Outsourcing Functions for Non-Channeling

CONTRACT BETWEEN
[AUTHORIZED RECIPIENT'S NAME]
AND
[CONTRACTOR'S NAME]
REGARDING OUTSOURCING
NONCRIMINAL JUSTICE ADMINISTRATIVE FUNCTIONS

This contract is entered into between **[insert Authorized Recipient's name and address]**, the Authorized Recipient, and **[insert Contractor's name and address]**, the Contractor, under the terms of which the Authorized Recipient is outsourcing the performance of noncriminal justice administrative functions involving the handling of criminal history record information (CHRI) pursuant to Title 28, Code of Federal Regulations, Part 906 and the Security and Management Control Outsourcing Standard (Outsourcing Standard) for Non-Channelers. The most current version of the Outsourcing Standard is incorporated by reference into this contract and appended hereto as Attachment "[insert]".

The Authorized Recipient's authority to submit fingerprints for noncriminal justice purposes and obtain the results of the fingerprint search, which may contain CHRI, is **[insert the legal citation of the statute or public law that requires or authorizes the Authorized Recipient to have access to CHRI]**. This authority requires or authorizes fingerprint-based background checks of **[insert all categories of current and prospective employees, licensees, or applicants for other benefits covered by the statute or public law]**.

The specific noncriminal justice administrative function to be performed by the Contractor that involve access to CHRI on behalf of the Authorized Recipient is to **[insert specific noncriminal justice administrative functions to be performed; i.e., missing dispositions, fitness determinations, storing criminal history record check results]**.

[Insert Contractor's name] will comply with the Outsourcing Standard for Non-Channelers requirements, to include the *CJIS Security Policy*, and other legal authorities to ensure adequate privacy and security of personally identifiable information (PII) and criminal history record check results related to this contract, and will ensure that all such data is returned to the Authorized Recipient as soon as no longer needed for the performance of contractual duties.

NOTE: A copy of the signature page with dates should be included with the contract.

Examples of Channeling Documentation

Authorized Recipient Sample Request Letter to Use a Channeler

REQUEST LETTER
FOR **[insert Authorized Recipient's name]** TO USE
[insert Contractor's name] AS A CHANNELER FOR THE SUBMISSION OF
AUTHORIZED NONCRIMINAL JUSTICE BACKGROUND CHECKS

[Date]

[Insert FBI Compact Officer's Name], FBI Compact Officer
FBI CJIS Division
1000 Custer Hollow Road, Module D3
Clarksburg, West Virginia 26306

Dear **[FBI Compact Officer's name]**:

[Insert Authorized Recipient's name and address], the Authorized Recipient, requests permission to outsource noncriminal justice administrative functions to FBI-approved Channeler, **[insert Contractor's name and address]**, the Contractor, to perform "Channeler" functions as set forth below. This request is made pursuant to Title 28, Code of Federal Regulations, Part 906 and the Security and Management Control Outsourcing Standard (Outsourcing Standard) for Channelers. **[Insert Authorized Recipient's name]**'s authority to submit fingerprints for noncriminal justice purposes and obtain the results of the fingerprint search, which may contain criminal history record information (CHRI), is pursuant to **[insert the legal citation of the statute or public law that requires or authorizes the Authorized Recipient to have access to CHRI]**. This authority requires or authorizes fingerprint-based background checks of **[insert all categories of current and prospective employees, licensees, or applicants for other benefits covered by the statute or public law]**.

[Insert Contractor's name] will serve as a "Channeler" on behalf of **[insert Authorized Recipient's name]**. The noncriminal justice administrative functions to be performed by the Channeler that may result in Channeler access to CHRI on behalf of **[insert Authorized Recipient's name]** are:

- Receive noncriminal justice applicant fingerprint submissions and collect associated fees;
- Ensure each fingerprint submission is properly and adequately completed;
- Electronically store and forward **[insert estimated number of annual submissions]** fingerprint transactions to the FBI's CJIS Division for national criminal history record checks;
- Receive electronic criminal history record check results from the FBI;
- Promptly disseminate all criminal history record check results to **[insert Authorized Recipient's name]** by **[insert means of dissemination – e.g. United States mail, e-mail, or posting to a web site]**; and
- Comply with all Outsourcing Standard for Channelers requirements.

Upon execution of the Contract, **[insert Authorized Recipient's name]** will take responsibility for **[insert Contractor's name]** compliance with the terms of the Contract, to include the Outsourcing Standard for Channelers, and will notify the FBI Compact Officer of any violations.

Sincerely,

[insert name]
[insert title]
[insert phone number]
[insert email address]
[insert fax number]

[insert ORI, if currently have one]

Sample FBI Response Letter for Channeler Request

[Date]

[Name]

[Position Title]

[Division]

[State Agency]

[Address]

[City, State and Zip Code]

Dear [Name]:

Reference is made to your request to outsource noncriminal justice administrative functions to **[insert Contractor's name]**, an FBI-approved Channeler. It is noted that your authority for access to the FBI criminal history record information (CHRI) is **[insert the statutory authority that requires or authorizes the Authorized Recipient to have access to CHRI]**.

In accordance with the National Crime Prevention and Privacy Compact Council's Final Rule entitled "Outsourcing of Noncriminal Justice Administrative Functions," (Title 28, Code of Federal Regulations, Part 906), outsourcing of noncriminal justice administrative functions is permitted under certain conditions when approved by the FBI Compact Officer. Accordingly, the **[insert Authorized Recipient's name]** is granted permissions to utilize **[insert Channeler's name]** to perform Channeler functions as set forth below. Please recognize that this approval is automatically rescinded should the **[insert Authorized Recipient's name]** lose its status as an Authorized Recipient or **[insert Channeler's name]** lose its status as an FBI-approved Channeler.

The **[insert Authorized Recipient's name]/[insert Contractor's name]** agreement shall, at a minimum, have incorporated by reference and appended thereto the current Security and Management control Outsourcing Standard for Channelers (Outsourcing Standard). In the event of a conflict between the terms of the **[insert Authorized Recipient's name]/[insert Contractor's name]** agreement, amendments to the agreement, and the Outsourcing Standard relating to the FBI-provided data, the terms of the Outsourcing Standard shall control.

The Channeler functions to be performed by **[insert Contractor's name]** pertain only to (1) fingerprint submissions to the FBI of **[insert authorized types of Authorized Recipients and how/why they are authorized to access CHRI]**, and (2) the concomitant dissemination of national fingerprint-based criminal history record check results. The Reason Fingerprinted field on the fingerprint submissions must be populated with "**[insert reason fingerprinted]**."

Pursuant to the Outsourcing Standard, the **[insert Authorized Recipient's name]** is responsible for the actions of the contractor and shall monitor the contractor's compliance to the terms and conditions of the Outsourcing Standard. As noted in the Outsourcing Standard, the FBI will perform limited auditing functions on behalf of the **[insert Authorized Recipient's name]**. Enclosed is a copy of the most current version of the Outsourcing Standard, dated **[insert date of current version]**.

Access to the FBI-maintained CHRI is subject to numerous restrictive laws and regulations. Dissemination of such information to a private entity is prohibited except as specifically authorized by federal law or regulation. Further, the exchange of CHRI is subject to cancellation if such unauthorized dissemination is made.

Should you have any questions regarding your responsibilities in relation to the outsourcing of noncriminal justice administrative functions, please do not hesitate to contact **[insert name of CJIS Division POC]** at **[insert telephone number]**, or via e-mail at **[insert e-mail address]** or me at **[insert telephone number]**, or via e-mail at **[insert e-mail address]**.

Respectfully,

[Insert FBI Compact Officer's name]

FBI Compact Officer

Enclosure

Note: Send a copy of the response to the FBI-approved Channeler.

Sample Language between the Authorized Recipient and Channeler regarding Noncriminal Justice Outsourcing Functions

CONTRACT BETWEEN
[AUTHORIZED RECIPIENT'S NAME]
AND
[CHANNELING CONTRACTOR'S NAME]
REGARDING OUTSOURCING
NONCRIMINAL JUSTICE ADMINISTRATIVE FUNCTIONS

This contract is entered into between **[insert Authorized Recipient's name and address]**, the Authorized Recipient, and **[insert Contractor's name and address]**, the Contractor, under the terms of which the Authorized Recipient is outsourcing the performance of noncriminal justice administrative functions involving the handling of criminal history record information (CHRI) pursuant to Title 28, Code of Federal Regulations, Part 906 and the Security and Management Control Outsourcing Standard (Outsourcing Standard) for Channelers. The most current version of the Outsourcing Standard for Channelers is incorporated by reference into this contract and appended hereto as Attachment "[insert]".

The Authorized Recipient's authority to submit fingerprints for noncriminal justice purposes and obtain the results of the fingerprint search, which may contain CHRI, is **[insert the legal citation of the statute or public law that requires or authorizes the Authorized Recipient to have access to CHRI]**. This authority requires or authorizes fingerprint-based background checks of **[insert all categories of current and prospective employees, licensees, or applicants for other benefits covered by the statute or public law]**.

The specific noncriminal justice administrative function to be performed by the Contractor that involve access to CHRI on behalf of the Authorized Recipient is to serve as an FBI-approved Channeler. The noncriminal justice administrative functions to be performed by the Channeler that may result in Channeler access to CHRI on behalf of **[insert Authorized Recipient's name]** are (1) Receive noncriminal justice applicant fingerprint submissions and collect associated fees; (2) Ensure each fingerprint submission is properly and adequately completed; (3) Electronically store and forward **[insert estimated number of annual submissions]** fingerprint transactions to the FBI's CJIS Division for national criminal history record checks; (4) Receive electronic criminal history record check results from the FBI; (5) Promptly disseminate all criminal history record check results to **[insert Authorized Recipient's name]** by **[insert means of dissemination – e.g. United States mail, e-mail, or posting to a web site]**; and (6) Comply with all Outsourcing Standard for Channelers requirements.

[NOTE: The FBI Compact Officer may also request the Authorized Recipient to provide the contract or portion(s) of the contract that sets forth the above language, the signature page(s), and the page with the effective date of the contract].

Outsourcing Audit Guidelines

If state or local ARs are authorized to conduct national fingerprint-based background checks based on a state or federal statute, the SCO/CA may not grant permission to outsource noncriminal justice administrative functions unless he/she has implemented a combined state/federal audit program to, at a minimum, triennially audit a representative sample of the Contractors and ARs engaging in outsourcing with the first of such audits to be conducted within one year of the date the Contractor first receives CHRI under an approved outsourcing agreement. A representative sample will be based on generally accepted statistical sampling methods.

Additionally, sections 2.05 of the Outsourcing Standards require certification that an audit was conducted with the Contractor within 90 days of the date the Contractor first receives CHRI under the approved outsourcing agreement. It should be noted that each of the Outsourcing Standards places the auditing responsibility on specific parties. Specifically, the FBI will, and the AR may, conduct an audit of the Contractor performing channeling functions and the FBI is required to certify to the FBI Compact Officer that an audit was conducted; whereas, the AR will certify to the SCO/CA that an audit was conducted of the Contractor performing Non-Channeling functions.

Sample Audit Methodology

The purpose of the audit is to assess compliance with applicable laws, policies, regulations, and rules which pertain to access to CHRI. The audit should be scoped to cover the following areas:

- adherence to Outsourcing Standard requirements;
- use of CHRI
- dissemination of CHRI
- physical and technical security of CHRI
- compliance with other applicable laws, policies, regulations, and rules.

States are encouraged to use the following sample methodology as a guide when creating the state audit process. In addition, Table 2-1 graphically displays the FBI CJIS Division's outsourcing audit methodology. For additional information relating to noncriminal justice agency audits, please refer to the Council's *Audit Guide* which may be found on the Law Enforcement Online Special Interest Group accessible through the Law Enforcement Enterprise Portal.

Pre-audit

Appropriate representatives from ARs and Contractors selected for audit are identified and notified to discuss an overview of the audit process and scheduling of audit activities. Requests for documentation such as copies of signed contracts occur during this phase. Additionally, points-of-contact are informed that pre-audit materials will be forwarded for review and completion. Pre-audit materials are useful for gathering pertinent information prior to on-site visits and may include high-level questionnaires that are used to formulate specific questions about agency processes, as well as data quality surveys comprised of a sampling of transactions or records that are used to validate agency processes.

On-Site Audit

Administrative interviews are conducted on-site with appropriate representatives from selected ARs and Contractors. Questions focus on capturing the specific processes used by agencies to meet Outsourcing Standard requirements. In addition, on-site validation of data quality surveys is conducted. Upon completion of the on-site visit, auditors make an initial determination of compliance and conduct an exit briefing with agency personnel. On-site audit activities also include the identification of any follow-up action items necessary to complete assessments.

Report

A draft audit report of findings and recommendations are completed and forwarded to AR and Contractor personnel responsible for oversight and compliance. Findings and recommendations are sufficiently detailed and directly correlate to specific policy requirements. The draft report solicits a response describing corrective actions and offering any additional comments. Upon receipt of the response, the audit report is finalized.

Sanctions

Final audit reports, which incorporate comments from ARs and Contractors, are forwarded to the appropriate sanctioning body for review. Upon review, the sanctioning body may consider requiring additional corrective actions or information. In addition, the sanctions process incorporates measures to elevate sanctions in a manner such that deficiencies are corrected and the risk of subsequent violations is adequately mitigated.

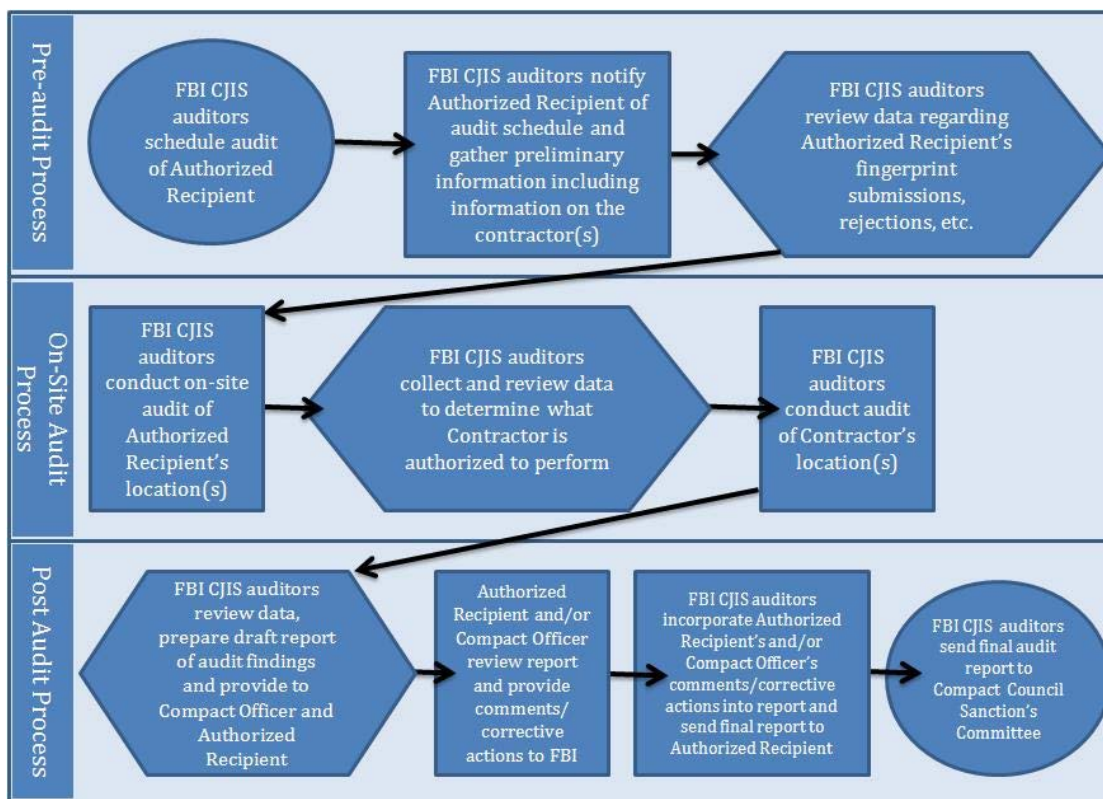


Table 2-1: Outsourcing Audit Methodology

Sample 90 day Audit Checklist for an Authorized Recipient

The Outsourcing Standard for Non-Channelers requires ARs who have been approved to outsource noncriminal justice administrative functions conduct an audit of the Contractor within 90 days of the date that the Contractor first receives CHRI under the approved outsourcing agreement. The following chart has been designed as a tool to assist ARs who are developing an audit process to comply with the 90 day audit requirement based on the Outsourcing Standard for Non-Channelers.

The chart outlines assessment items which have been grouped topically. References to the specific requirements in the Outsourcing Standard for Non-Channelers and the *CJIS Security Policy* have also been provided for each assessment item. Depending on the function outsourced and the specifics of the process, all of the requirements listed may not be applicable.

Sample 90 day Audit Checklist for an Authorized Recipient

Contractor Assessment	Reference	Yes	No	N/A
	OS-Outsourcing Standard for Non-Channelers CSP-CJIS Security Policy			
Policy References				
a. Copy of current Outsourcing Standard for Non-Channelers	OS 2.02, 2.03, 2.05, 2.07, 3.02, 3.03, 5.03, 6.02, 7.01, 8.01a, 9.01, 9.04, 11.05, 11.06			
b. Copy of current <i>CJIS Security Policy</i>	OS 2.03b, 2.03c, 3.01, 3.02, 3.03, 7.01, 7.02, 9.02			
Security Program				
a. Authorized Recipient (AR) approved minimum requirements for content of Security Program	OS 3.02			
b. Implementation of security requirements	OS 3.02, 3.03 a-d			
c. Reporting procedures for security violations	OS 3.03(c), 8.0			
Security Training Program				
a. AR approved	OS 3.04			
b. Training prior to appointment or assignment	OS 3.04			
c. Training upon receipt of changes	OS 3.04			
d. Annual refresher training	OS 3.04			
Site Security				
a. Available for announced/unannounced audits	OS 3.05			
b. Physically secure location	OS 4.01, 7.02a			
Use and Maintenance of CHRI				
a. Maintained in accordance with contract and does not exceed period of time AR is authorized to maintain	OS 3.07			
b. Used only in accordance with contract and AR's authority	OS 2.03, 3.01			
Dissemination				
a. AR approved in accordance with contract and AR's authority	OS 5.01			
b. Compliant with laws, rules, and regulations[1]	OS 5.01			
c. Log captured required information and retained for a minimum of 365 days	OS 3.08, 5.02			
Personnel Security				
a. Criminal background checks on all Contractor and approved sub-Contractor personnel with access to CHRI conducted prior to access	OS 6.01			
b. Confirmation of understanding by employee(s)	OS 6.02			
c. List of personnel with access to CHRI	OS 6.03			
d. Updates to list of personnel changes within 24 hours of changes	OS 6.03			

Based on OS for Non-Channelers dated 11/06/14 and CJIS Security Policy 5.3 dated 8/4/14

Page 1 of 2

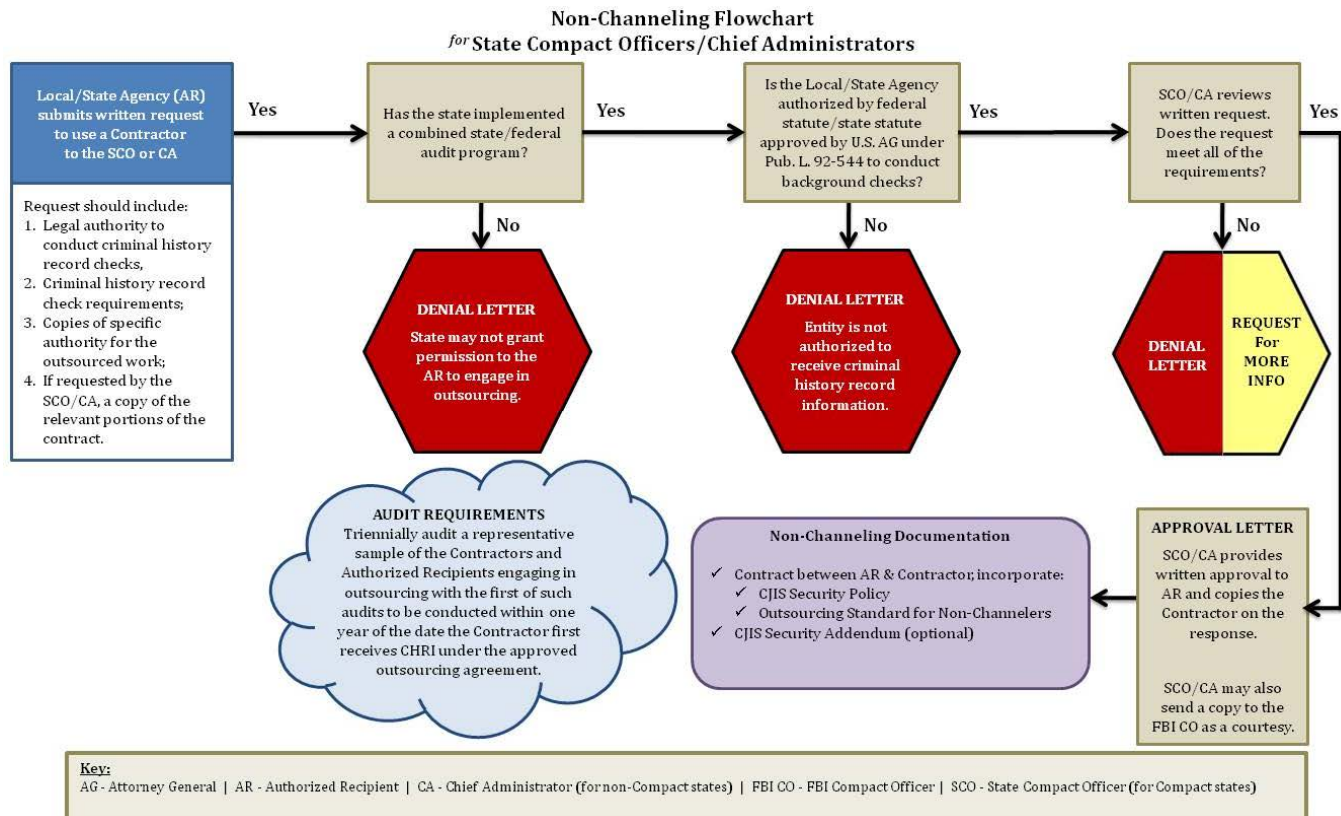
[1] Applicable laws, rules, and regulations regarding the dissemination of national CHRI include Title 28, United States Code, Section 534; Title 28, Code of Federal Regulations, Section 50.12 (b) and Part 906.

Contractor Assessment	Reference	Yes	No	N/A
	OS-Outsourcing Standard for Non-Channelers CSP-CJIS Security Policy			
Security Violations				
a. Develop and maintain written security violation plan	OS 8.01a, 2.07, 3.03			
b. Policy for disciplinary action	OS 8.01a			
c. Immediate suspension pending investigation	OS 8.01b			
d. Immediate report	OS 8.01c			
d. Follow-up report	OS 8.01c			
Security on Systems Processing CHRI				
a. Current topological drawing	OS 2.04			
b. Firewalls	OS 7.01a, CSP 5.10			
c. Encryption	OS 7.01b, CSP 5.5.2.4, 5.10.1.2			
f. Virus protection on networks processing CHRI	CSP 5.10.4.2			
g. User identification	CSP 5.6			
h. Authentication of user identification	CSP 5.6			
i. Advanced authentication when accessing via the Internet	CSP 5.6			
j. Audit trails	CSP 5.4.6			
Media Destruction				
a. Hard copy	OS 7.02c, CSP 5.8.4			
b. Electronic media	OS 7.02, CSP 5.8.3			

Based on OS for Non-Channelers dated 11/6/14 and CJIS Security Policy 5.3 dated 8/4/14

Page 2 of 2

Non-Channeling Flowchart for SCO/CA



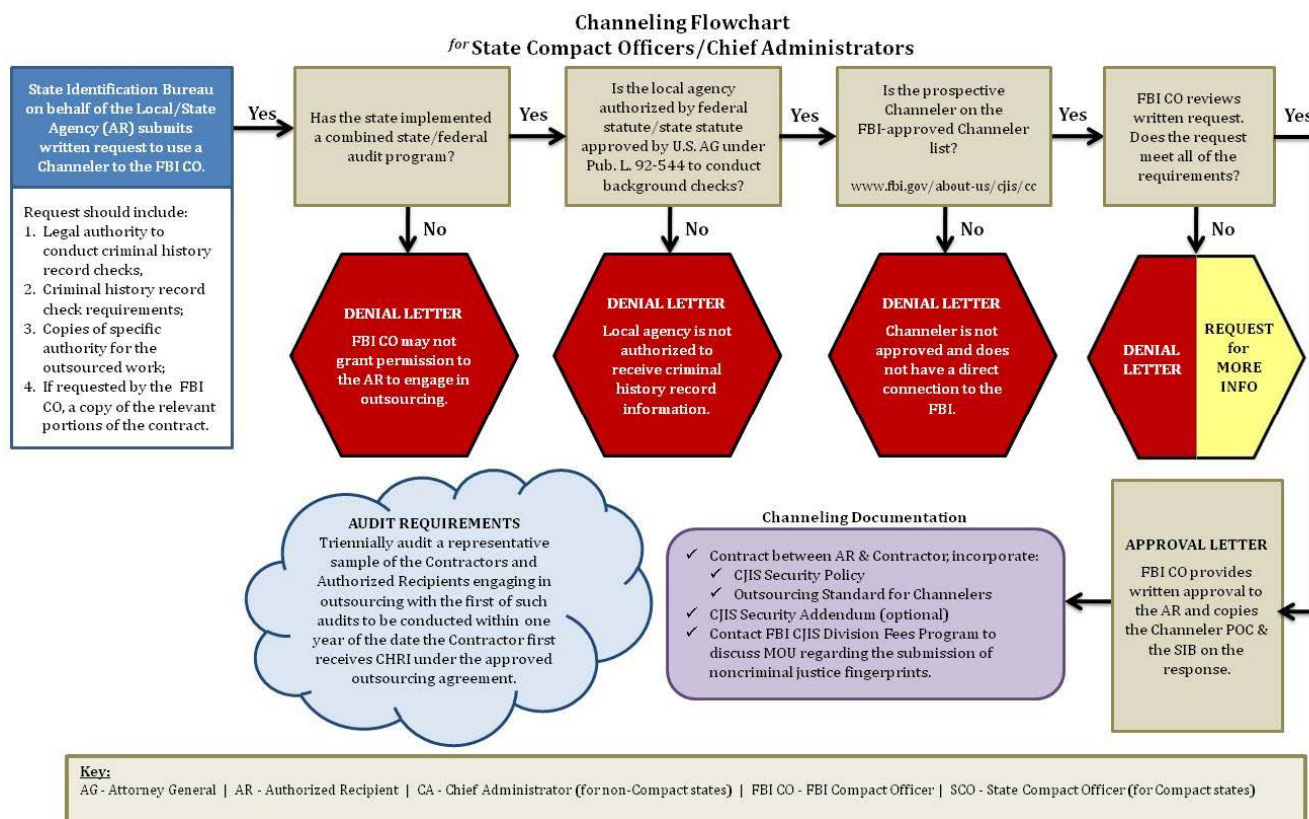
Non-Channeling Checklist for SCO/CA

Non-Channeling Checklist for State Compact Officers/Chief Administrators

- ☐ Receives a written request from an Agency requesting approval to outsource noncriminal justice administrative functions to a Contractor on behalf of the Agency.
- ☐ Must have implemented a combined state/federal audit program to, at a minimum, triennially audit a representative sample of the Contractors and ARs engaging in outsourcing with the first of such audits to be conducted within one year of the date the Contractor first receives CHRI under the approved outsourcing agreement.
- ☐ Review the incoming request letter to include copies of the specific authority for the outsourced work, the state or federal requirement for the criminal history record check, and/or, if requested, a copy of relevant portions of the contract. The legal authority should be referenced in the written request.
- ☐ Ensure that the most current versions of both the Outsourcing Standard for Non-Channelers (www.fbi.gov/about-us/cjis/cc/) and the *CJIS Security Policy* (www.fbi.gov/about-us/cjis/cjis-security-policy/cjis-security-policy/view) are incorporated by reference and appended to the contract at the time of the contract and/or option renewal.
- ☐ Contract specifies the terms and conditions of CHRI access as specified in the Outsourcing Standard for Non-Channelers and the *CJIS Security Policy*:
 - ____ Limit the use of such information to the purposes for which it is provided.
 - ____ Limit the retention of the information.
 - ____ Prohibit the dissemination of the information except as specifically authorized by federal and state laws, regulations and standards as well as rules, procedures and standards established by the Compact Council and the U.S. AG.
 - ____ Ensure the security and confidentiality of the information to include confirmation that the Contractor is authorized to receive CHRI.
 - ____ Provide audits and sanctions.
 - ____ Provide conditions for termination of the contract.
 - ____ Maintain up-to-date records of Contractor personnel that have access to CHRI.
 - ____ Ensure Contractor personnel comply with the Outsourcing Standard for Non-Channelers and the *CJIS Security Policy*.
- ☐ Upon completion of the review, the SCO/CA will prepare and send an approval or denial letter to the Agency with a copy to the prospective Contractor.
- ☐ The SCO/CA may visit the Contractor's facilities for announced and unannounced audits and security inspections.
- ☐ The SCO/CA will review and approve the Contractor's Security Program.
- ☐ Received certification that the AR conducted an audit of the Contractor within 90 days of the date the Contractor first receives CHRI under the approved outsourcing agreement.

NOTE: State Compact Officer (SCO) of Party [Compact] States
Chief Administrator (CA) of non-Party States

Channeling Flowchart for SCO/CA



Channeling Checklist for SCO/CA

Channeling Checklist for State Compact Officers/Chief Administrators

- ☐ Receives a written request from an Agency requesting approval to outsource the **submission of fingerprints and receipt of the corresponding CHRI** to a Channeler on behalf of the Agency.
- ☐ Must have implemented a combined state/federal audit program to, at a minimum, triennially audit a representative sample of the Contractors and ARs engaging in outsourcing with the first of such audits to be conducted within one year of the date the Contractor first receives CHRI under the approved outsourcing agreement.
- ☐ Review the incoming request letter to include copies of the specific authority for the outsourced work, the state or federal requirement for the criminal history record check, and/or, if requested, a copy of relevant portions of the contract. The legal authority should be referenced in the written request.
- ☐ Verifies that the Channeler is listed on the FBI-approved Channeler list. This most current list may be found on the web at: www.fbi.gov/about-us/cjis/cc/current-initiatives/list-of-fbi-approved-channelers.
- ☐ SCO/CA on behalf of the Local/State Agency (AR) submits a written request to the FBI Compact Officer (CO) to outsource the **submission of fingerprints and receipt of the corresponding CHRI** to a Channeler. The letter should contain the same information as the request from the Local/State Agency.
- ☐ AR will enter into a contract with the Channeler and will ensure that the most current version of both the Outsourcing Standard for Channelers (www.fbi.gov/about-us/cjis/cc/) and the *CJIS Security Policy* (www.fbi.gov/about-us/cjis/cjis-security-policy/cjis-security-policy/view) are incorporated by reference and appended to the contract at the time of the contract and/or option renewal.
- ☐ Contract specifies the terms and conditions of CHRI access as specified in the Outsourcing Standard for Channelers and the *CJIS Security Policy*:
 - _____ Limit the use of such information to the purposes for which it is provided.
 - _____ Limit the retention of the information.
 - _____ Prohibit the dissemination of the information except as specifically authorized by federal and state laws, regulations and standards as well as rules, procedures and standards established by the Compact Council and the U.S. AG.
 - _____ Ensure the security and confidentiality of the information to include confirmation that the Contractor is authorized to receive CHRI.
 - _____ Provide audits and sanctions.
 - _____ Provide conditions for termination of the contract.
 - _____ Maintain up-to-date records of Contractor personnel that have access to CHRI.
 - _____ Ensure Contractor personnel comply with the Outsourcing Standard for Channelers and the *CJIS Security Policy*
- ☐ Upon completion of the review, the FBI CO will prepare and send an approval or denial letter to the SCO/CA with a copy to the prospective Channeler and the AR.
- ☐ The SCO/CA will notify the Local/State Agency in writing whether the request was approved or denied.
- ☐ The SCO/CA and the AR may elect to visit the Contractor's facilities for announced and unannounced audits and security inspections.
- ☐ The SCO/CA and the AR may elect to review the Contractor's Security Program.
- ☐ The SCO/CA will add to audit schedule: triennially audit a representative sample of Contractors and ARs engaging in outsourcing with the first of such audits to be conducted within one year of the date the Contractor first receives CHRI under the approved outsourcing agreement.

NOTE: State Compact Officer (SCO) of Party [Compact] States
Chief Administrator (CA) of non-Party States

Frequently Asked Questions

Non-Channeler FAQ's

- 1. Does an Authorized Recipient have to use the same Contractor to perform noncriminal justice administrative functions (i.e., storage, missing disposition, etc.) that it is using as a Channeler?**

No. An Authorized Recipient may use an FBI-approved Channeler to perform both functions but are not required to do so. An Authorized Recipient may choose any of the FBI-approved Channelers to perform the Channeling function and any Non-Channeling Contractor to perform the noncriminal justice administrative function(s). However, two separate request letters shall be submitted for approval (one for channeling and one for Non-Channeling) to the State Compact Officer/Chief Administrator/FBI Compact Officer) and preferably two separate contracts issued.

- 2. If an Authorized Recipient has a contract with an FBI-approved Channeler to channel fingerprints and store the CHRI on their behalf, does the Authorized Recipient have to touch the CHRI prior to the storage?**

Yes. Channeling fingerprints and Non-Channeling noncriminal justice administrative functions are two separate and distinct services an Authorized Recipient is outsourcing with a company. Pursuant to the Title 28, Code of Federal Regulations, Part 906 and the Security and Management Control Outsourcing Standard for Channelers, a Channeler shall expeditiously disseminate the criminal history record check results. An FBI-approved Channeler's role is simply to act as an "expeditor" on behalf of the Authorized Recipient.

- 3. Can a Contractor performing noncriminal justice administrative functions on behalf of an Authorized Recipient share the CHRI with another Contractor working with the Authorized Recipient?**

No. The Authorized Recipient is the only entity authorized to share CHRI with a Contractor in accordance with the Security and Management Control Outsourcing Standards for Non-Channelers.

Channeler FAQ's

1. Does a Channeler request letter have to be mailed to the FBI?

No. An Authorized Recipient requesting to use an FBI-approved Channeler can mail, fax, or email the request to the FBI Compact Officer.

2. Can a Channeler submit fingerprints directly to the FBI for a state agency and bypass the state?

No. A state agency that is authorized by statute to submit fingerprints to the FBI must be submitted by the state repository unless the state repository is outsourcing the Channeling function.

3. After the Channeler receives the criminal history record information (CHRI) from the FBI (on behalf of the Authorized Recipient) can the Authorized Recipient have the Channeler send the CHRI directly to another Contractor?

No. The Channeler is simply an expeditor of the CHRI and shall only send the CHRI response back to the Authorized Recipient.

4. Is there a list of potential customers that can be provided to the Channelers?

The FBI conducts national fingerprint-based criminal history record checks for noncriminal justice purposes when authorized by federal statute or executive order, state statute that has been approved by the United States Attorney General, or United States Attorney General Order. The FBI System of Records Notice (SORN) is published in the *Federal Register* (64FR52343) and sets out the routine uses of records maintained in the Fingerprint Identification Records Systems, including categories of users and the purposes of such uses. There is no central listing of "Authorized Recipients."

5. Can a Channeler publicize information on its website that it is an FBI-approved Channeler?

News releases or notices may be published on a Channeler's website only after approval from the FBI Contracting Officer.

6. Can a company outside the United States submit fingerprints to the FBI through an FBI-approved Channeler?

No. A non-U.S. company has no authority to submit fingerprints and receive CHRI.

Recommended Online Reference Materials

- List of FBI-Approved Channelers –
www.fbi.gov/about-us/cjis/cc/current-initiatives/list-of-fbi-approved-channelers-1
- Security and Management Control Outsourcing Standard for Channelers (current version) –
www.fbi.gov/about-us/cjis/cc/
- Security and Management Control Outsourcing Standard for Non-Channelers (current version)–
www.fbi.gov/about-us/cjis/cc/
- FBI *Criminal Justice Information Systems (CJIS) Security Policy* (current version) –
www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view
- Missouri State Highway Patrol CJIS Division, Policy Compliance Program –
www.mshp.dps.missouri.gov/MSHPWeb/Publications/Handbooks-Manuals/documents/SHP-185PCRReferenceManual.pdf
- Georgia Crime Information Center –
www.ga.cogentid.com/GA_DOCS_html/Outsourcing_Narrative_09102007.htm and
<http://gbi.georgia.gov/non-criminal-justice-agencies>
- FBI Biometric Center of Excellence –
www.fbibiospecs.org
- Electronic Biometric Transmission Specification (EBTS) –
www.fbibiospecs.org/ebts.html

Definitions

The following definitions are provided in the State Guide as a matter of information and may be found in Section 1.0 of the Council's Outsourcing Standards for Channelers and Non-Channelers. Many of the definitions appear in both of the Outsourcing Standards; however, if a definition applies to only a specific standard it is noted in bold text.

- **Access to CHRI** means to view or make use of CHRI obtained from the III System but excludes direct access to the III System by computer terminal or other automated means by Contractors other than those that may be contracted by the FBI or state criminal history record repositories or as provided by Title 34, U.S.C., Section 40314 (b), (formerly cited as Title 42, U.S.C., Section 14614(b)).
- **Authorized Recipient (AR)** means (1) a nongovernmental entity authorized by federal statute or federal executive order to receive CHRI for noncriminal justice purposes, or (2) a government agency authorized by federal statute, federal executive order, or state statute which has been approved by the United States Attorney General to receive CHRI for noncriminal justice purposes.
- **Authorized Recipient's Information Security Officer** means the individual who shall ensure technical compliance with all applicable elements of the **Outsourcing Standard for Channelers**.
- **Chief Administrator** means the primary administrator of a Nonparty State=s criminal history record repository or a designee of such administrator who is a regular full-time employee of the repository, which is also referred to as the State Identification Bureau (SIB) Chief.
- **Criminal History Record Information (CHRI)**, as referred to in Article I(4) of the Compact, means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, or release; but does not include identification information such as fingerprint records if such information does not indicate involvement of the individual with the criminal justice system.
- **Criminal History Record Check (CHRC)**, for purposes of the Outsourcing Standards only, means an authorized noncriminal justice fingerprint-based search of a state criminal history record repository and/or the FBI system.
- **CJIS Systems Agency (CSA)**, as provided in Section 1.4 of the FBI Criminal Justice Information Services (CJIS) Division's Advisory Policy Board Bylaws (dated 12/2/2009), means a criminal justice agency which has overall responsibility for the administration and usage of CJIS Division Programs within a state, district, territory, or foreign country. This includes any federal agency

that meets the definition and provides services to other federal agencies and/or whose users reside in multiple states or territories. This definition is applicable to the **Outsourcing Standard for Channelers**.

- **CJIS Systems Officer (CSO)**, as provided in Section 1.5 of the CJIS Advisory Policy Board Bylaws (dated 12/2/2009), means the individual employed by the CJIS Systems Agency who is responsible for monitoring system use, enforcing system discipline and security, and assuring that CJIS operating procedures are followed by all users as well as other related duties outlined by the user agreements with the FBI's CJIS Division. (This title was formerly referred to as the Control Terminal Officer or the Federal Service Coordinator). This definition is applicable to the **Outsourcing Standard for Channelers**.
- **Compact Officer**, as provided in Article I(2) of the Compact, means (A) with respect to the Federal Government, an official [FBI Compact Officer] so designated by the Director of the FBI [to administer and enforce the Compact among federal agencies], or (B) with respect to a Party State, the chief administrator of the State's criminal history record repository or a designee of the chief administrator who is a regular full-time employee of the repository.
- **Contractor**, under the **Outsourcing Standard for Channelers**, means a government agency, a private business, non-profit organization or individual, that is not itself an Authorized Recipient with respect to the particular noncriminal justice purpose, who has entered into a contract with an Authorized Recipient to perform channeler functions requiring access to CHRI. Under the Outsourcing Standard for Channelers, a Contractor serves as a Channeler and has direct connectivity to the CJIS Wide Area Network (WAN) for the purpose of electronic submission of fingerprints to and the receipt of CHRI from the FBI on behalf of an Authorized Recipient.
- **Contractor**, under the **Outsourcing Standard for Non-Channelers**, means a government agency, a private business, non-profit organization or individual, that is not itself an Authorized Recipient with respect to the particular noncriminal justice purpose, who has entered into a contract with an Authorized Recipient to perform noncriminal justice administrative functions requiring access to CHRI.
- **Contractor's Security Officer** means the individual accountable for the management of the Contractor's security program.
- **Dissemination** means the disclosure of III CHRI by an Authorized Recipient to an authorized Contractor, or by the Contractor to another Authorized Recipient consistent with the Contractor's responsibilities and with limitations imposed by federal and state laws, regulations, and standards as well as rules, procedures, and standards established by the Compact Council and the United States Attorney General.

- **Noncriminal Justice Administrative Functions** means the routine noncriminal justice administrative functions relating to the processing of CHRI, to include but not limited to the following:
 - (1) Making fitness determinations/recommendations
 - (2) Obtaining missing dispositions
 - (3) Disseminating CHRI as authorized by Federal statute, Federal Executive Order, or State statute approved by the United States Attorney General
 - (4) Other authorized activities relating to the general handling, use, and storage of CHRI
- **Noncriminal Justice Purposes**, as provided in Article I(18) of the Compact, means uses of criminal history records for purposes authorized by federal or state law other than purposes relating to criminal justice activities, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.
- **Outsourcing Standard (OS)** means a document approved by the Compact Council after consultation with the United States Attorney General which is to be incorporated by reference into a contract between an Authorized Recipient and a Contractor. The Outsourcing Standard authorizes access to CHRI for noncriminal justice purposes, limits the use of the information to the purposes for which it is provided, prohibits retention and/or dissemination except as specifically authorized, ensures the security and confidentiality of the information, provides for audits and sanctions, provides conditions for termination of the contract, and contains such other provisions as the Compact Council may require.
- **Physically Secure Location** means a facility or an area, a room, or a group of rooms, within a facility with both the physical and personnel security controls sufficient to protect CHRI and associated information systems.
- **Positive Identification**, as provided in Article I(20) of the Compact, means a determination, based upon a comparison of fingerprints¹ or other equally reliable biometric identification techniques, that the subject of a record search is the same person as the subject of a criminal history record or records indexed in the III System. Identifications based solely upon a comparison of subjects' names or other non-unique identification characteristics or numbers, or combinations thereof, shall not constitute positive identification.
- **Public Carrier Network** means a telecommunications infrastructure consisting of network components that are not owned, operated, and managed solely by the agency using that network, i.e., any telecommunications infrastructure which supports public users other than those of the agency using that network. Examples of a public carrier network include but are not limited to the following: Dial-up and Internet connections, network connections to Verizon, network connections to AT&T, ATM Frame Relay clouds, wireless networks, wireless links, and

¹ The Compact Council currently defines positive identification for noncriminal justice purposes as identification based upon a qualifying ten-rolled or qualifying ten-flat fingerprint submission. Further information concerning positive identification may be obtained from the FBI Compact Council office.

cellular telephones. A public carrier network provides network services to the public; not just to the single agency using that network.

- **Security Violation** means the failure to prevent or failure to institute safeguards to prevent access, use, retention, or dissemination of CHRI in violation of: (A) federal or state law, regulation, or Executive Order; or (B) a rule, procedure, or standard established by the Compact Council and the United States Attorney General.

Appendices

Appendix

A **Interim Final Rule: Outsourcing of Noncriminal Justice Administrative Functions**
Federal Register/Volume 69, Number 241/December 16, 2004

B **Final Rule: Outsourcing of Noncriminal Justice Administrative Functions**
Federal Register/Volume 70, Number 240/December 15, 2005

C **Security and Management Control Outsourcing Standard for Channelers**
Current Version dated November 6, 2014

D **Security and Management Control Outsourcing Standard for Non-Channelers**
Current Version dated November 6, 2014



Appendix A

Interim Final Rule:

Outsourcing of Noncriminal Justice Administrative Functions

Federal Register/Volume 69, Number 241/December 16, 2004

INSERT Document

Page 1 of 3

INSERT Document

Page 2 of 3

INSERT Document

Page 3 of 3



Appendix B

Final Rule: Outsourcing of Noncriminal Justice Administrative Functions
Federal Register/Volume 70, Number 240/December 15, 2005

INSERT DOCUMENT

Page 1 of 1



Appendix C

Security and Management Control Outsourcing Standard for Channelers
Current Version dated November 6, 2014

INSERT DOCUMENT

Page 1 of 13

INSERT DOCUMENT

Page 2 of 13

INSERT DOCUMENT

Page 3 of 13

INSERT DOCUMENT

Page 4 of 13

INSERT DOCUMENT

Page 5 of 13

INSERT DOCUMENT

Page 6 of 13

INSERT DOCUMENT

Page 7 of 13

INSERT DOCUMENT

Page 8 of 13

INSERT DOCUMENT

Page 9 of 13

INSERT DOCUMENT

Page 10 of 13

INSERT DOCUMENT

Page 11 of 13

INSERT DOCUMENT

Page 12 of 13

INSERT DOCUMENT

Page 13 of 13



Appendix D

Security and Management Control Outsourcing Standard for Non-Channelers
Current Version dated November 6, 2014

INSERT Document

Page 1 of 13

INSERT Document

Page 2 of 13

INSERT Document

Page 3 of 13

INSERT Document

Page 4 of 13

INSERT Document

Page 5 of 13

INSERT Document

Page 6 of 13

INSERT Document

Page 7 of 13

INSERT Document

Page 8 of 13

INSERT Document

Page 9 of 13

INSERT Document

Page 10 of 13

INSERT Document

Page 11 of 13

INSERT Document

Page 12 of 13

INSERT Document

Page 13 of 13

Joe Lombardo
Governor



**Nevada Department of
Public Safety**
Records, Communications and Compliance

George Togliatti
Director

Sheri Brueggemann
Deputy Director

Erica Souza-Llamas
Division Administrator

Records, Communications and Compliance Division

333 West Nye Lane, Suite 100

Carson City, Nevada 89706

Telephone (775) 684-6262 – Fax (775) 684-6265

www.rccd.nv.gov

Address

Agency name
Contact

Dear Noncriminal Justice Compliance Team:

The following is an updated authorized personnel list for **AGENCY NAME and ACCOUNT**

<u>Authorized Individual</u>	<u>Title</u>	<u>Role</u>	<u>Training Date</u>
Dumpty, Humpty	Director	Making hiring decision	01/15/2015
Duckling, Ugly	Assistant	File confidential files	03/07/2015
Racer, Speed	HR Analyst	Review application	01/04/2016

If you have any questions, you can reach me at **AGENCY PHONE NUMBER** and **EMAIL**.

Humpty Dumpty, Director
DPS RCCD

School Year	Master District Code	District Name	State District Code	School Code
2627	01	Churchill	01	202
2627	01	Churchill	01	205
2627	01	Churchill	01	206
2627	01	Churchill	01	207
2627	01	Churchill	01	301
2627	01	Churchill	01	401
2627	01	Churchill	01	902
2627	02	Clark County	02	060
2627	02	Clark County	02	061
2627	02	Clark County	02	062
2627	02	Clark County	02	064
2627	02	Clark County	02	065
2627	02	Clark County	02	066
2627	02	Clark County	02	067
2627	02	Clark County	02	068
2627	02	Clark County	02	069
2627	02	Clark County	02	070
2627	02	Clark County	02	071
2627	02	Clark County	02	072
2627	02	Clark County	02	073
2627	02	Clark County	02	074
2627	02	Clark County	02	075
2627	02	Clark County	02	076
2627	02	Clark County	02	077
2627	02	Clark County	02	078
2627	02	Clark County	02	079
2627	02	Clark County	02	080
2627	02	Clark County	02	081
2627	02	Clark County	02	082
2627	02	Clark County	02	083
2627	02	Clark County	02	084
2627	02	Clark County	02	085
2627	02	Clark County	02	086
2627	02	Clark County	02	088

2627	02	Clark County	02	089
2627	02	Clark County	02	090
2627	02	Clark County	02	091
2627	02	Clark County	02	094
2627	02	Clark County	02	095
2627	02	Clark County	02	096
2627	02	Clark County	02	097
2627	02	Clark County	02	098
2627	02	Clark County	02	099
2627	02	Clark County	02	100
2627	02	Clark County	02	101
2627	02	Clark County	02	103
2627	02	Clark County	02	104
2627	02	Clark County	02	105
2627	02	Clark County	02	106
2627	02	Clark County	02	107
2627	02	Clark County	02	108
2627	02	Clark County	02	109
2627	02	Clark County	02	110
2627	02	Clark County	02	111
2627	02	Clark County	02	112
2627	02	Clark County	02	113
2627	02	Clark County	02	114
2627	02	Clark County	02	115
2627	02	Clark County	02	116
2627	02	Clark County	02	117
2627	02	Clark County	02	118
2627	02	Clark County	02	119
2627	02	Clark County	02	120
2627	02	Clark County	02	121
2627	02	Clark County	02	122
2627	02	Clark County	02	123
2627	02	Clark County	02	124
2627	02	Clark County	02	125
2627	02	Clark County	02	126

2627	02	Clark County	02	127
2627	02	Clark County	02	128
2627	02	Clark County	02	129
2627	02	Clark County	02	130
2627	02	Clark County	02	131
2627	02	Clark County	02	132
2627	02	Clark County	02	133
2627	02	Clark County	02	134
2627	02	Clark County	02	135
2627	02	Clark County	02	136
2627	02	Clark County	02	137
2627	02	Clark County	02	138
2627	02	Clark County	02	139
2627	02	Clark County	02	140
2627	02	Clark County	02	141
2627	02	Clark County	02	142
2627	02	Clark County	02	143
2627	02	Clark County	02	144
2627	02	Clark County	02	145
2627	02	Clark County	02	146
2627	02	Clark County	02	147
2627	02	Clark County	02	148
2627	02	Clark County	02	149
2627	02	Clark County	02	150
2627	02	Clark County	02	151
2627	02	Clark County	02	152
2627	02	Clark County	02	153
2627	02	Clark County	02	154
2627	02	Clark County	02	155
2627	02	Clark County	02	156
2627	02	Clark County	02	157
2627	02	Clark County	02	158
2627	02	Clark County	02	159
2627	02	Clark County	02	160
2627	02	Clark County	02	161

2627	02	Clark County	02	162
2627	02	Clark County	02	163
2627	02	Clark County	02	164
2627	02	Clark County	02	165
2627	02	Clark County	02	166
2627	02	Clark County	02	167
2627	02	Clark County	02	168
2627	02	Clark County	02	169
2627	02	Clark County	02	170
2627	02	Clark County	02	171
2627	02	Clark County	02	172
2627	02	Clark County	02	173
2627	02	Clark County	02	174
2627	02	Clark County	02	175
2627	02	Clark County	02	176
2627	02	Clark County	02	177
2627	02	Clark County	02	178
2627	02	Clark County	02	179
2627	02	Clark County	02	180
2627	02	Clark County	02	181
2627	02	Clark County	02	182
2627	02	Clark County	02	183
2627	02	Clark County	02	184
2627	02	Clark County	02	185
2627	02	Clark County	02	186
2627	02	Clark County	02	187
2627	02	Clark County	02	188
2627	02	Clark County	02	189
2627	02	Clark County	02	190
2627	02	Clark County	02	191
2627	02	Clark County	02	192
2627	02	Clark County	02	193
2627	02	Clark County	02	194
2627	02	Clark County	02	195
2627	02	Clark County	02	196

2627	02	Clark County	02	197
2627	02	Clark County	02	198
2627	02	Clark County	02	199
2627	02	Clark County	02	200
2627	02	Clark County	02	201
2627	02	Clark County	02	202
2627	02	Clark County	02	203
2627	02	Clark County	02	204
2627	02	Clark County	02	205
2627	02	Clark County	02	206
2627	02	Clark County	02	207
2627	02	Clark County	02	208
2627	02	Clark County	02	209
2627	02	Clark County	02	210
2627	02	Clark County	02	211
2627	02	Clark County	02	212
2627	02	Clark County	02	213
2627	02	Clark County	02	214
2627	02	Clark County	02	215
2627	02	Clark County	02	216
2627	02	Clark County	02	217
2627	02	Clark County	02	218
2627	02	Clark County	02	219
2627	02	Clark County	02	220
2627	02	Clark County	02	221
2627	02	Clark County	02	222
2627	02	Clark County	02	223
2627	02	Clark County	02	224
2627	02	Clark County	02	225
2627	02	Clark County	02	226
2627	02	Clark County	02	227
2627	02	Clark County	02	228
2627	02	Clark County	02	230
2627	02	Clark County	02	231
2627	02	Clark County	02	232

2627	02	Clark County	02	233
2627	02	Clark County	02	234
2627	02	Clark County	02	235
2627	02	Clark County	02	236
2627	02	Clark County	02	237
2627	02	Clark County	02	238
2627	02	Clark County	02	239
2627	02	Clark County	02	241
2627	02	Clark County	02	242
2627	02	Clark County	02	243
2627	02	Clark County	02	244
2627	02	Clark County	02	245
2627	02	Clark County	02	246
2627	02	Clark County	02	247
2627	02	Clark County	02	248
2627	02	Clark County	02	249
2627	02	Clark County	02	250
2627	02	Clark County	02	251
2627	02	Clark County	02	252
2627	02	Clark County	02	253
2627	02	Clark County	02	254
2627	02	Clark County	02	255
2627	02	Clark County	02	256
2627	02	Clark County	02	257
2627	02	Clark County	02	258
2627	02	Clark County	02	259
2627	02	Clark County	02	260
2627	02	Clark County	02	261
2627	02	Clark County	02	262
2627	02	Clark County	02	263
2627	02	Clark County	02	264
2627	02	Clark County	02	265
2627	02	Clark County	02	266
2627	02	Clark County	02	267
2627	02	Clark County	02	268

2627	02	Clark County	02	269
2627	02	Clark County	02	270
2627	02	Clark County	02	271
2627	02	Clark County	02	272
2627	02	Clark County	02	273
2627	02	Clark County	02	274
2627	02	Clark County	02	275
2627	02	Clark County	02	276
2627	02	Clark County	02	277
2627	02	Clark County	02	278
2627	02	Clark County	02	279
2627	02	Clark County	02	280
2627	02	Clark County	02	281
2627	02	Clark County	02	282
2627	02	Clark County	02	283
2627	02	Clark County	02	284
2627	02	Clark County	02	285
2627	02	Clark County	02	286
2627	02	Clark County	02	287
2627	02	Clark County	02	289
2627	02	Clark County	02	290
2627	02	Clark County	02	291
2627	02	Clark County	02	292
2627	02	Clark County	02	293
2627	02	Clark County	02	294
2627	02	Clark County	02	295
2627	02	Clark County	02	296
2627	02	Clark County	02	297
2627	02	Clark County	02	298
2627	02	Clark County	02	300
2627	02	Clark County	02	301
2627	02	Clark County	02	302
2627	02	Clark County	02	303
2627	02	Clark County	02	304
2627	02	Clark County	02	305

2627	02	Clark County	02	306
2627	02	Clark County	02	307
2627	02	Clark County	02	308
2627	02	Clark County	02	309
2627	02	Clark County	02	310
2627	02	Clark County	02	311
2627	02	Clark County	02	312
2627	02	Clark County	02	313
2627	02	Clark County	02	314
2627	02	Clark County	02	316
2627	02	Clark County	02	317
2627	02	Clark County	02	318
2627	02	Clark County	02	319
2627	02	Clark County	02	320
2627	02	Clark County	02	321
2627	02	Clark County	02	322
2627	02	Clark County	02	323
2627	02	Clark County	02	324
2627	02	Clark County	02	325
2627	02	Clark County	02	326
2627	02	Clark County	02	327
2627	02	Clark County	02	328
2627	02	Clark County	02	329
2627	02	Clark County	02	330
2627	02	Clark County	02	331
2627	02	Clark County	02	332
2627	02	Clark County	02	333
2627	02	Clark County	02	334
2627	02	Clark County	02	335
2627	02	Clark County	02	336
2627	02	Clark County	02	337
2627	02	Clark County	02	338
2627	02	Clark County	02	339
2627	02	Clark County	02	341
2627	02	Clark County	02	342

2627	02	Clark County	02	343
2627	02	Clark County	02	344
2627	02	Clark County	02	345
2627	02	Clark County	02	346
2627	02	Clark County	02	347
2627	02	Clark County	02	348
2627	02	Clark County	02	349
2627	02	Clark County	02	350
2627	02	Clark County	02	352
2627	02	Clark County	02	353
2627	02	Clark County	02	354
2627	02	Clark County	02	355
2627	02	Clark County	02	356
2627	02	Clark County	02	357
2627	02	Clark County	02	359
2627	02	Clark County	02	360
2627	02	Clark County	02	361
2627	02	Clark County	02	362
2627	02	Clark County	02	368
2627	02	Clark County	02	369
2627	02	Clark County	02	401
2627	02	Clark County	02	402
2627	02	Clark County	02	403
2627	02	Clark County	02	404
2627	02	Clark County	02	405
2627	02	Clark County	02	406
2627	02	Clark County	02	408
2627	02	Clark County	02	409
2627	02	Clark County	02	410
2627	02	Clark County	02	411
2627	02	Clark County	02	412
2627	02	Clark County	02	414
2627	02	Clark County	02	415
2627	02	Clark County	02	416
2627	02	Clark County	02	417

2627	02	Clark County	02	418
2627	02	Clark County	02	420
2627	02	Clark County	02	421
2627	02	Clark County	02	422
2627	02	Clark County	02	423
2627	02	Clark County	02	424
2627	02	Clark County	02	425
2627	02	Clark County	02	426
2627	02	Clark County	02	427
2627	02	Clark County	02	428
2627	02	Clark County	02	429
2627	02	Clark County	02	430
2627	02	Clark County	02	431
2627	02	Clark County	02	432
2627	02	Clark County	02	433
2627	02	Clark County	02	434
2627	02	Clark County	02	435
2627	02	Clark County	02	501
2627	02	Clark County	02	601
2627	02	Clark County	02	602
2627	02	Clark County	02	603
2627	02	Clark County	02	604
2627	02	Clark County	02	607
2627	02	Clark County	02	608
2627	02	Clark County	02	609
2627	02	Clark County	02	611
2627	02	Clark County	02	612
2627	02	Clark County	02	618
2627	02	Clark County	02	619
2627	02	Clark County	02	620
2627	02	Clark County	02	623
2627	02	Clark County	02	624
2627	02	Clark County	02	625
2627	02	Clark County	02	626
2627	02	Clark County	02	627

2627	02	Clark County	02	628
2627	02	Clark County	02	716
2627	02	Clark County	02	777
2627	02	Clark County	02	901
2627	02	Clark County	02	902
2627	02	Clark County	02	903
2627	02	Clark County	02	904
2627	02	Clark County	02	905
2627	02	Clark County	02	906
2627	02	Clark County	02	907
2627	02	Clark County	02	910
2627	02	Clark County	02	911
2627	02	Clark County	02	912
2627	02	Clark County	02	913
2627	02	Clark County	02	916
2627	02	Clark County	02	917
2627	02	Clark County	02	919
2627	02	Clark County	02	922
2627	02	Clark County	02	923
2627	02	Clark County	02	924
2627	02	Clark County	02	926
2627	02	Clark County	02	927
2627	02	Clark County	02	928
2627	02	Clark County	02	932
2627	02	Clark County	02	933
2627	02	Clark County	02	935
2627	02	Clark County	02	936
2627	02	Clark County	02	939
2627	02	Clark County	02	940
2627	02	Clark County	02	941
2627	02	Clark County	02	953
2627	02	Clark County	02	954
2627	02	Clark County	02	955
2627	02	Clark County	02	956
2627	02	Clark County	02	957

2627	02	Clark County	02	958
2627	02	Clark County	02	960
2627	02	Clark County	02	965
2627	03	Douglas	03	201
2627	03	Douglas	03	202
2627	03	Douglas	03	206
2627	03	Douglas	03	207
2627	03	Douglas	03	209
2627	03	Douglas	03	210
2627	03	Douglas	03	301
2627	03	Douglas	03	302
2627	03	Douglas	03	501
2627	03	Douglas	03	502
2627	03	Douglas	03	503
2627	03	Douglas	03	504
2627	03	Douglas	03	601
2627	03	Douglas	03	901
2627	03	Douglas	03	903
2627	03	Douglas	03	950
2627	04	Elko	04	104
2627	04	Elko	04	105
2627	04	Elko	04	107
2627	04	Elko	04	108
2627	04	Elko	04	111
2627	04	Elko	04	120
2627	04	Elko	04	202
2627	04	Elko	04	203
2627	04	Elko	04	204
2627	04	Elko	04	205
2627	04	Elko	04	206
2627	04	Elko	04	207
2627	04	Elko	04	208
2627	04	Elko	04	209
2627	04	Elko	04	210
2627	04	Elko	04	211

2627	04	Elko	04	213
2627	04	Elko	04	501
2627	04	Elko	04	502
2627	04	Elko	04	503
2627	04	Elko	04	504
2627	04	Elko	04	505
2627	04	Elko	04	506
2627	04	Elko	04	507
2627	04	Elko	04	601
2627	04	Elko	04	602
2627	04	Elko	04	603
2627	04	Elko	04	604
2627	04	Elko	04	605
2627	04	Elko	04	606
2627	04	Elko	04	607
2627	04	Elko	04	610
2627	04	Elko	04	902
2627	04	Elko	04	904
2627	04	Elko	04	905
2627	04	Elko	04	908
2627	05	Esmeralda	05	101
2627	05	Esmeralda	05	102
2627	05	Esmeralda	05	501
2627	06	Eureka	06	101
2627	06	Eureka	06	103
2627	06	Eureka	06	601
2627	07	Humboldt	07	101
2627	07	Humboldt	07	103
2627	07	Humboldt	07	104
2627	07	Humboldt	07	105
2627	07	Humboldt	07	106
2627	07	Humboldt	07	201
2627	07	Humboldt	07	203
2627	07	Humboldt	07	205
2627	07	Humboldt	07	301

2627	07	Humboldt	07	302
2627	07	Humboldt	07	501
2627	07	Humboldt	07	601
2627	07	Humboldt	07	903
2627	07	Humboldt	07	930
2627	08	Lander	08	201
2627	08	Lander	08	302
2627	08	Lander	08	601
2627	08	Lander	08	602
2627	08	Lander	08	902
2627	09	Lincoln	09	102
2627	09	Lincoln	09	201
2627	09	Lincoln	09	202
2627	09	Lincoln	09	203
2627	09	Lincoln	09	301
2627	09	Lincoln	09	302
2627	09	Lincoln	09	501
2627	09	Lincoln	09	601
2627	09	Lincoln	09	602
2627	09	Lincoln	09	603
2627	09	Lincoln	09	903
2627	10	Lyon	10	201
2627	10	Lyon	10	202
2627	10	Lyon	10	203
2627	10	Lyon	10	205
2627	10	Lyon	10	206
2627	10	Lyon	10	208
2627	10	Lyon	10	209
2627	10	Lyon	10	210
2627	10	Lyon	10	211
2627	10	Lyon	10	302
2627	10	Lyon	10	303
2627	10	Lyon	10	304
2627	10	Lyon	10	305
2627	10	Lyon	10	601

2627	10	Lyon	10	602
2627	10	Lyon	10	603
2627	10	Lyon	10	604
2627	10	Lyon	10	605
2627	10	Lyon	10	902
2627	10	Lyon	10	907
2627	10	Lyon	10	950
2627	10	Lyon	10	960
2627	11	Mineral	11	201
2627	11	Mineral	11	202
2627	11	Mineral	11	203
2627	11	Mineral	11	601
2627	11	Mineral	11	925
2627	12	Nye	12	102
2627	12	Nye	12	103
2627	12	Nye	12	105
2627	12	Nye	12	106
2627	12	Nye	12	108
2627	12	Nye	12	201
2627	12	Nye	12	202
2627	12	Nye	12	206
2627	12	Nye	12	207
2627	12	Nye	12	210
2627	12	Nye	12	301
2627	12	Nye	12	311
2627	12	Nye	12	312
2627	12	Nye	12	313
2627	12	Nye	12	315
2627	12	Nye	12	316
2627	12	Nye	12	601
2627	12	Nye	12	602
2627	12	Nye	12	603
2627	12	Nye	12	604
2627	12	Nye	12	605
2627	12	Nye	12	606

2627	12	Nye	12	607
2627	12	Nye	12	609
2627	12	Nye	12	902
2627	13	Carson City	13	201
2627	13	Carson City	13	202
2627	13	Carson City	13	203
2627	13	Carson City	13	204
2627	13	Carson City	13	207
2627	13	Carson City	13	209
2627	13	Carson City	13	211
2627	13	Carson City	13	212
2627	13	Carson City	13	301
2627	13	Carson City	13	302
2627	13	Carson City	13	501
2627	14	Pershing	14	101
2627	14	Pershing	14	201
2627	14	Pershing	14	301
2627	14	Pershing	14	601
2627	14	Pershing	14	903
2627	14	Pershing	14	991
2627	15	Storey	15	101
2627	15	Storey	15	102
2627	15	Storey	15	301
2627	15	Storey	15	601
2627	16	Washoe County	16	201
2627	16	Washoe County	16	202
2627	16	Washoe County	16	203
2627	16	Washoe County	16	204
2627	16	Washoe County	16	205
2627	16	Washoe County	16	206
2627	16	Washoe County	16	207
2627	16	Washoe County	16	208
2627	16	Washoe County	16	209
2627	16	Washoe County	16	210
2627	16	Washoe County	16	211

2627	16	Washoe County	16	212
2627	16	Washoe County	16	213
2627	16	Washoe County	16	214
2627	16	Washoe County	16	215
2627	16	Washoe County	16	216
2627	16	Washoe County	16	218
2627	16	Washoe County	16	219
2627	16	Washoe County	16	220
2627	16	Washoe County	16	221
2627	16	Washoe County	16	222
2627	16	Washoe County	16	223
2627	16	Washoe County	16	224
2627	16	Washoe County	16	225
2627	16	Washoe County	16	226
2627	16	Washoe County	16	227
2627	16	Washoe County	16	228
2627	16	Washoe County	16	229
2627	16	Washoe County	16	230
2627	16	Washoe County	16	231
2627	16	Washoe County	16	232
2627	16	Washoe County	16	233
2627	16	Washoe County	16	234
2627	16	Washoe County	16	235
2627	16	Washoe County	16	237
2627	16	Washoe County	16	238
2627	16	Washoe County	16	239
2627	16	Washoe County	16	240
2627	16	Washoe County	16	241
2627	16	Washoe County	16	242
2627	16	Washoe County	16	243
2627	16	Washoe County	16	244
2627	16	Washoe County	16	245
2627	16	Washoe County	16	246
2627	16	Washoe County	16	251
2627	16	Washoe County	16	256

2627	16	Washoe County	16	257
2627	16	Washoe County	16	258
2627	16	Washoe County	16	259
2627	16	Washoe County	16	260
2627	16	Washoe County	16	261
2627	16	Washoe County	16	262
2627	16	Washoe County	16	263
2627	16	Washoe County	16	264
2627	16	Washoe County	16	265
2627	16	Washoe County	16	266
2627	16	Washoe County	16	267
2627	16	Washoe County	16	268
2627	16	Washoe County	16	269
2627	16	Washoe County	16	270
2627	16	Washoe County	16	271
2627	16	Washoe County	16	272
2627	16	Washoe County	16	273
2627	16	Washoe County	16	274
2627	16	Washoe County	16	275
2627	16	Washoe County	16	276
2627	16	Washoe County	16	278
2627	16	Washoe County	16	279
2627	16	Washoe County	16	280
2627	16	Washoe County	16	281
2627	16	Washoe County	16	282
2627	16	Washoe County	16	301
2627	16	Washoe County	16	303
2627	16	Washoe County	16	304
2627	16	Washoe County	16	305
2627	16	Washoe County	16	306
2627	16	Washoe County	16	307
2627	16	Washoe County	16	308
2627	16	Washoe County	16	309
2627	16	Washoe County	16	310
2627	16	Washoe County	16	311

2627	16	Washoe County	16	312
2627	16	Washoe County	16	315
2627	16	Washoe County	16	316
2627	16	Washoe County	16	317
2627	16	Washoe County	16	318
2627	16	Washoe County	16	319
2627	16	Washoe County	16	320
2627	16	Washoe County	16	321
2627	16	Washoe County	16	322
2627	16	Washoe County	16	501
2627	16	Washoe County	16	502
2627	16	Washoe County	16	503
2627	16	Washoe County	16	504
2627	16	Washoe County	16	505
2627	16	Washoe County	16	507
2627	16	Washoe County	16	508
2627	16	Washoe County	16	509
2627	16	Washoe County	16	510
2627	16	Washoe County	16	511
2627	16	Washoe County	16	601
2627	16	Washoe County	16	602
2627	16	Washoe County	16	603
2627	16	Washoe County	16	605
2627	16	Washoe County	16	606
2627	16	Washoe County	16	607
2627	16	Washoe County	16	608
2627	16	Washoe County	16	609
2627	16	Washoe County	16	610
2627	16	Washoe County	16	611
2627	16	Washoe County	16	900
2627	16	Washoe County	16	904
2627	16	Washoe County	16	911
2627	16	Washoe County	16	917
2627	16	Washoe County	16	921
2627	16	Washoe County	16	922

2627	16	Washoe County	16	923
2627	16	Washoe County	16	930
2627	17	White Pine County School District	17	101
2627	17	White Pine County School District	17	103
2627	17	White Pine County School District	17	201
2627	17	White Pine County School District	17	203
2627	17	White Pine County School District	17	204
2627	17	White Pine County School District	17	301
2627	17	White Pine County School District	17	502
2627	17	White Pine County School District	17	601
2627	17	White Pine County School District	17	903
2627	17	White Pine County School District	17	904
2627	17	White Pine County School District	17	930
2627	17	White Pine County School District	17	999
2627	38	Freedom Classical Academy	18	435
2627	39	Legacy Traditional School	18	438
2627	39	Legacy Traditional School	18	439
2627	39	Legacy Traditional School	18	440
2627	43	Futuro Academy	18	100
2627	44	Mater Academy of Northern Nevada	18	437
2627	45	EarlyChildhood District	45	100
2627	45	EarlyChildhood District	45	101
2627	45	EarlyChildhood District	45	102
2627	45	EarlyChildhood District	45	105
2627	45	EarlyChildhood District	45	111
2627	45	EarlyChildhood District	45	115
2627	45	EarlyChildhood District	45	123
2627	45	EarlyChildhood District	45	124
2627	45	EarlyChildhood District	45	125
2627	45	EarlyChildhood District	45	126
2627	45	EarlyChildhood District	45	127
2627	45	EarlyChildhood District	45	128
2627	45	EarlyChildhood District	45	500
2627	46	DPAC Nevada	18	100
2627	47	Sports Leadership and Management Academy	18	200

2627	48	Equipo Academy	18	300
2627	49	Mater Academy of Nevada	18	434
2627	49	Mater Academy of Nevada	18	433
2627	49	Mater Academy of Nevada	18	432
2627	49	Mater Academy of Nevada	18	433
2627	49	Mater Academy of Nevada	18	434
2627	50	Amplus Academy	18	431
2627	50	Amplus Academy	18	432
2627	51	Founders Academy of Las Vegas	18	430
2627	52	Leadership Academy of Nevada	18	429
2627	54	Learning Bridge	18	428
2627	55	Doral Academy	18	200
2627	55	Doral Academy	18	201
2627	55	Doral Academy	18	202
2627	55	Doral Academy	18	203
2627	55	Doral Academy	18	204
2627	57	Honors Academy of Literature	18	424
2627	58	Pinecrest Academy of Nevada	18	422
2627	58	Pinecrest Academy of Nevada	18	423
2627	58	Pinecrest Academy of Nevada	18	425
2627	58	Pinecrest Academy of Nevada	18	427
2627	58	Pinecrest Academy of Nevada	18	428
2627	58	Pinecrest Academy of Nevada	18	429
2627	58	Pinecrest Academy of Nevada	18	430
2627	59	Somerset Academy of Las Vegas	18	119
2627	59	Somerset Academy of Las Vegas	18	120
2627	59	Somerset Academy of Las Vegas	18	121
2627	59	Somerset Academy of Las Vegas	18	122
2627	59	Somerset Academy of Las Vegas	18	123
2627	59	Somerset Academy of Las Vegas	18	124
2627	59	Somerset Academy of Las Vegas	18	125
2627	60	Explore Knowledge Academy	18	401
2627	61	Discovery Preparatory Academy	18	415
2627	61	Discovery Preparatory Academy	18	417
2627	62	Do & Be Arts Academy of Excellence	18	101

2627	64	Rainbow Dreams Early Learning Academy	18	87
2627	65	Oasis Academy	18	414
2627	66	Doral Academy of Northern Nevada	18	436
2627	67	The Delta Academy	18	201
2627	68	Elko Institute for Academic Achievement	18	410
2627	69	Innovations International Charter School	18	101
2627	69	Innovations International Charter School	18	201
2627	72	Quest Academy	18	416
2627	74	Imagine School Mountain View	18	418
2627	75	FuturEdge Academy	18	401
2627	76	Alpine Academy	18	412
2627	77	Odyssey Charter School	18	401
2627	78	Silver Sands Montessori	18	411
2627	79	Independence HS	20	903
2627	81	Nevada State High School	18	101
2627	81	Nevada State High School	18	102
2627	81	Nevada State High School	18	103
2627	81	Nevada State High School	18	104
2627	81	Nevada State High School	18	106
2627	81	Nevada State High School	18	107
2627	81	Nevada State High School	18	108
2627	81	Nevada State High School	18	109
2627	84	Davidson Academy	19	406
2627	85	Nevada Connections Academy	18	405
2627	86	Nevada Virtual Charter School	18	404
2627	87	Coral Academy of Science Las Vegas	18	310
2627	87	Coral Academy of Science Las Vegas	18	311
2627	87	Coral Academy of Science Las Vegas	18	312
2627	87	Coral Academy of Science Las Vegas	18	313
2627	87	Coral Academy of Science Las Vegas	18	314
2627	87	Coral Academy of Science Las Vegas	18	315
2627	87	Coral Academy of Science Las Vegas	18	316
2627	89	Beacon Academy of Nevada	18	409
2627	92	WYLEES	18	201
2627	95	Southern Nevada Trades High School	18	301

2627	96	Thrive Point Academy of Nevada	18	601
2627	97	Vegas Vista Academy	18	101
2627	98	Nevada Classical Academy Elko	18	101
2627	101	Nevada Rise Academy	18	101
2627	104	Nevada State High School II	18	101
2627	105	Signature Preparatory	18	101
2627	106	Pinecrest Academy of Northern Nevada	18	101
2627	107	Explore Academy	18	100
2627	110	CIVICA Academy	18	100
2627	113	Young Womens Leadership Academy of Las Vegas	18	100
2627	115	Strong Start Academy	18	100
2627	127	Academies of Math and Science	18	100
2627	300	Kesher Academy	22	100

State School Code	CEEB Number	Name	Abbreviated Name
1202		Northside Early Learning Center	Northside Early Learning
1205		E C Best Elementary	Best ES
1206		Lahontan Elementary School	Lahontan ES
1207		Numa Elementary School	Numa ES
1301		Churchill County Middle School	Churchill MS
1401	290060	Churchill County High School	Churchill HS
1902		Churchill County Adult Ed	Churchill Adult Ed
2060		Thompson, Tyrone ES	Thompson T ES
2061		Abston, Sandra B ES	Abston ES
2062		Jenkins, Earl N ES	Jenkins ES
2064		Ellis, Robert & Sandy ES	Ellis ES
2065		Ortwein, Dennis ES	Ortwein ES
2066		Barber, Shirley A ES	Barber ES
2067		Divich, Kenneth ES	Divich ES
2068		Jones Blackhurst, Jan L ES	Jones Blackhurst ES
2069		Vassiliadis, Billy & Rosemary ES	Vassiliadis ES
2070		Berkley, Shelley ES	Berkley ES
2071		Stevens, Josh ES	Stevens ES
2072		Mathis, Dr. Beverly S ES	Mathis ES
2073		Heard, Lomie G ES	Heard ES
2074		Snyder, Don & Dee ES	Snyder D ES
2075		NW Career-Technical Academy ES	NWCTA ES
2076		Duncan, Ruby ES	Duncan ES
2077		Wallin, Shirley & Bill ES	Wallin ES
2078		Stuckey, Evelyn ES	Stuckey ES
2079		Keller, Charlotte & Jerry ES	Keller ES
2080		Fine, Mark L ES	Fine ES
2081		Bozarth, Henry & Evelyn ES	Bozarth ES
2082		Triggs, Vincent L ES	Triggs ES
2083		O Roarke, Thomas ES	ORoarke ES
2084		Reedom, Carolyn S ES	Reedom ES
2085		Diaz, Ruben P ES	Diaz ES
2086		Scott, Jesse D ES	Scott ES
2088		Southeast Career Technical Academy PK	SECTA PK

2089		West, Dr. Charles I. Preparatory Academy ES	West Prep ES
2090		Smalley, James E & A Rae ES	Smalley
2091		Perkins, Dr Claude G ES	Perkins C ES
2094		Dickens, D L Dusty ES	Dickens ES
2095		Bailey, Sister Robert Joseph ES	Bailey ES
2096		Roundy, Dr C Owen ES	Roundy ES
2097		Forbuss, Robert L ES	Forbuss ES
2098		Steele, Judith D ES	Steele ES
2099		Schorr, Steve ES	Schorr ES
2100		Ward, Kitty McDonough ES	Ward Kitty ES
2101		Blue Diamond ES	Blue Diamond ES
2103		Lundy, Earl B ES	Lundy ES
2104		Reid, Harry ES	Reid ES
2105		King Jr , Martin Luther ES	King Martin ES
2106		Deskin, Ruthe ES	Deskin
2107		Kim, Frank ES	Kim ES
2108		Beatty, John R ES	Beatty J ES
2109		Christensen, M J ES	Christensen ES
2110		Parson, Claude & Stella ES	Parson ES
2111		Dooley, John ES	Dooley ES
2112		Mendoza, John F ES	Mendoza ES
2113		McMillan, James B ES	McMillan ES
2114		Perkins, Ute ES	Perkins U ES
2115		Lynch, Ann ES	Lynch ES
2116		Woolley, Gwendolyn ES	Woolley ES
2117		Lunt, Robert ES	Lunt ES
2118		Eisenberg, Dorothy ES	Eisenberg ES
2119		Fong, Wing and Lilly ES	Fong ES
2120		Gibson, James ES	Gibson ES
2121		Wynn, Elaine ES	Wynn ES
2122		Hill, Charlotte ES	Hill ES
2123		Jacobson, Walter ES	Jacobson ES
2124		Derfelt, Herbert A ES	Derfelt ES
2125		Cunningham, Cynthia ES	Cunningham ES
2126		Cox, David M ES	Cox D ES

2127		Treem, Harriet ES	Treem ES
2128		Rundle, Richard ES	Rundle ES
2129		Herr, Helen ES	Herr ES
2130		Dailey, Jack ES	Dailey ES
2131		Adams, Kirk ES	Adams ES
2132		May, Ernest ES	May ES
2133		Kahre, Marc ES	Kahre ES
2134		Katz, Edythe & Lloyd ES	Katz ES
2135		Jydstrup, Helen ES	Jydstrup ES
2136		King, Martha P ES	King Martha ES
2137		Bartlett, Selma F ES	Bartlett ES
2138		Bendorf, Patricia A ES	Bendorf ES
2139		Thorpe, Jim ES	Thorpe ES
2140		Antonello, Lee ES	Antonello ES
2141		Lummis, William ES	Lummis ES
2142		Wiener, Jr , Louis ES	Wiener ES
2143		Fitzgerald, H P ES	Fitzgerald ES
2144		Lowman, Mary & Zel ES	Lowman ES
2145		Piggott Academy ES	Piggott ACAD ES
2146		Newton, Uli ES	Newton ES
2147		Bruner, Lucile ES	Bruner ES
2148		Bryan, Richard H ES	Bryan Richard ES
2149		Wilhelm, Elizabeth ES	Wilhelm ES
2150		Roberts, Aggie ES	Roberts ES
2151		Allen, Dean LaMar ES	Allen ES
2152		Wolfe, Eva ES	Wolfe ES
2153		Goldfarb, Daniel ES	Goldfarb ES
2154		Vanderburg, John ES	Vanderburg ES
2155		Cambeiro, Arturo ES	Cambeiro ES
2156		Bryan, Roger M ES	Bryan Roger ES
2157		Bonner, John W ES	Bonner ES
2158		Cartwright, Roberta C ES	Cartwright ES
2159		Bowler, Joseph L ES	Bowler Joseph ES
2160		Rhodes, Betsy ES	Rhodes ES
2161		Guy, Addeliar D III ES	Guy ES

2162		Morrow, Sue H ES	Morrow ES
2163		Bunker, Berkeley L ES	Bunker ES
2164		Elizondo, Raul P ES	Elizondo ES
2165		Cortez, Manuel J ES	Cortez ES
2166		Lamping, Frank ES	Lamping ES
2167		Garehime, Edith ES	Garehime ES
2168		Hayes, Keith C & Karen W ES	Hayes ES
2169		Kesterson, Lorna J ES	Kesterson ES
2170		Neal, Joseph M ES	Neal ES
2171		Carl, Kay ES	Carl ES
2172		Darnell, Marshall C ES	Darnell ES
2173		Heckethorn, Howard E ES	Heckethorn ES
2174		Rogers, Lucille S ES	Rogers ES
2175		Snyder, William E ES	Snyder W ES
2176		Twitchell, Neil C ES	Twitchell ES
2177		Watson, Fredric W ES	Watson ES
2178		Alamo, Tony ES	Alamo ES
2179		Brookman, Eileen B ES	Brookman ES
2180		Cozine, Steve and Linda ES	Cozine ES
2181		Gehring, Roger D Acad of Science & Technology ES	Gehring ACAD ES
2182		Iverson, Mervin ES	Iverson ES
2183		Walker, J Marlan Int'l School ES	Walker ES
2184		Connors, Eileen ES	Connors ES
2185		Givens, Linda Rankin ES	Givens ES
2186		Goolsby, Judy & John L ES	Goolsby ES
2187		Hummel, John R ES	Hummel ES
2188		Scherkenbach, William & Mary ES	Scherkenbach ES
2189		Simmons, Eva G ES	Simmons ES
2190		Tanaka, Wayne N ES	Tanaka ES
2191		Tartan, John ES	Tartan ES
2192		Thiriot, Joseph E ES	Thiriot ES
2193		Batterman, Kathy L ES	Batterman ES
2194		Ries, Aldeane Comito ES	Ries ES
2195		Hickey, Liliam Lujan ES	Hickey ES
2196		Jeffers, Jay W ES	Jeffers ES

2197		Goynes, Theron H & Naomi D ES	Goynes ES
2198		Thompson, Sandra L ES	Thompson ES
2199		Hayden, Don E ES	Hayden ES
2200		Wright, William V ES	Wright ES
2201		Ronzone, Bertha ES	Ronzone ES
2202		Hoggard, Mabel ES	Hoggard ES
2203		Ronnow, C C ES	Ronnow ES
2204		Squires, C P ES	Squires ES
2205		Crestwood ES	Crestwood ES
2206		Gilbert, CVT ES	Gilbert ES
2207		Hancock, Doris ES	Hancock ES
2208		Griffith, E W ES	Griffith ES
2209		Herron, Fay ES	Herron ES
2210		Hewetson, Halle ES	Hewetson ES
2211		Booker, Kermit R Sr ES	Booker ES
2212		Earl, Ira J ES	Earl I ES
2213		Manch, J E ES	Manch ES
2214		Ullom, J M ES	Ullom ES
2215	991930	Miller, John F	Miller John F
2216		Park, John S ES	Park ES
2217		Mackey, Jo ES	Mackey ES
2218		McWilliams, J T ES	McWilliams ES
2219		Toland, Helen Anderson Intl Academy	Toland ES
2220		Dearing, Laura ES	Dearing ES
2221		Rowe, Lewis E ES	Rowe ES
2222		Lincoln ES	Lincoln ES
2223		Craig, Lois ES	Craig ES
2224		Williams, Wendell ES	Williams W ES
2225		Cahlan, Marion ES	Cahlan ES
2226		Kelly, Matt ES	Kelly ES
2227		Early Childhood ES	Clark Early Childhood
2228		Mountain View ES	Mountain View ES
2230		Taylor, Glen C ES	Taylor G ES
2231		Adcock, O K ES	Adcock ES
2232		Paradise Prof Dev ES	Paradise ES

2233		Culley, Paul E ES	Culley ES
2234		McCall, Quannah ES	McCall ES
2235		Red Rock ES	Red Rock ES
2236		Bell, Rex ES	Bell ES
2237		Lake, Robert E ES	Lake ES
2238		Warren, Rose ES	Warren ES
2239		Thomas, Ruby S ES	Thomas ES
2241		Sunrise Acres ES	Sunrise Acres ES
2242		Williams, Tom ES	Williams T ES
2243		Twin Lakes ES	Twin Lakes ES
2244		Pittman, Vail ES	Pittman ES
2245		Vegas Verdes ES	Vegas Verdes ES
2246		Bracken, Walter ES	Bracken ES
2247		Wasden, Howard ES	Wasden ES
2248		Beckley, Will ES	Beckley ES
2249		McCaw, Gordon ES	McCaw ES
2250		Mitchell, Andrew ES	Mitchell ES
2251		Sewell, C T ES	Sewell ES
2252		Indian Springs ES	Indian Springs ES
2253		Priest, Richard C ES	Priest ES
2254		Taylor, Robert L ES	Taylor R ES
2255		Virgin Valley ES	Virgin Valley ES
2256		Whitney ES	Whitney ES
2257		Ferron, William E ES	Ferron ES
2258		Ward, Gene ES	Gene Ward ES
2259		Wengert, Cyril ES	Wengert ES
2260		Tate, Myrtle ES	Tate ES
2261		Harmon, Harley ES	Harmon ES
2262		Harris, George E ES	Harris ES
2263		Diskin, P A ES	Diskin ES
2264		Smith, Helen M ES	Smith Helen ES
2265		Tomiyasu, Bill Y ES	Tomiyasu ES
2266		Dondero, Harvey N ES	Dondero ES
2267		Edwards, Elbert ES	Edwards ES
2268		French, Doris ES	French ES

2269		Decker, C H ES	Decker ES
2270		Long, Walter V ES	Long ES
2271		Bilbray, James ES	Bilbray ES
2272		Frias, Charles & Phyllis ES	Frias ES
2273		Hollingsworth, Howard ES	Hollingsworth ES
2274		Miller, Sandy Searles ES	Miller Sandy ES
2275		Gragson, Oran K ES	Gragson ES
2276		Galloway, Fay ES	Galloway ES
2277		Mack, Nate ES	Mack ES
2278		Gray, R Guild ES	Gray ES
2279		Bowler, Grant ES	Bowler Grant ES
2280		Bass, John C ES	Bass ES
2281		Martinez, Reynaldo L ES	Martinez ES
2282		Moore, William K ES	Moore ES
2283		Ober, D'Vorre & Hal ES	Ober ES
2284		Smith, Hal ES	Smith Hal ES
2285		Tarr, Sheila Academy of Int'l Studies ES	Tarr ES
2286		Staton, Ethel W ES	Staton ES
2287		Wolff, Elise L ES	Wolff ES
2289		Petersen, Dean ES	Petersen ES
2290		Tobler, R E ES	Tobler ES
2291		Sandy Valley ES	Sandy Valley ES
2292		Bennett, William G ES	Bennett William ES
2293		Cox, Clyde C ES	Cox C ES
2294		Stanford ES	Stanford ES
2295		Reed, Doris M ES	Reed ES
2296		Earl, Marion B ES	Earl M ES
2297		Hinman, Edna F ES	Hinman ES
2298		McDoniel, Estes M ES	McDoniel ES
2300		Detwiler, Ollie ES	Detwiler ES
2301		Von Tobel, Ed MS	Von Tobel MS
2302		Garside, Frank F JHS	Garside
2303		Hyde Park MS	Hyde Park MS
2304		Cashman, James MS	Cashman MS
2305		Smith, J D MS	Smith MS

2306		Brinley, J Harold MS	Brinley MS
2307		Bridger, Jim MS	Bridger MS
2308		Fremont, John C Professional Dev MS	Fremont MS
2309		Knudson, K O Academy of the Arts	Knudson MS
2310		Gibson, Robert O MS Leadership Academy	Gibson MS
2311		Martin, Roy W MS	Martin MS
2312		Orr, William E MS	Orr MS
2313		Burkholder, Lyal Academy of Environmental Science	Burkholder MS
2314		Woodbury, C W MS	Woodbury MS
2316		Cannon, Helen C JHS	Cannon JHS
2317		Guinn, Kenny C MS	Guinn MS
2318		Garrett, Elton M JHS	Garrett
2319		Brown, B Mahlon JHS	Brown JHS
2320	290253	Sandy Valley J-SHS	Sandy Valley JSHS
2321	290126	Laughlin J-SHS	Laughlin JSHS
2322		O'Callaghan, Mike MS i3 Learn Academy	O'Callaghan i3 ACAD
2323		Johnson, Walter JHS Academy of Int'l Studies	Johnson JHS
2324		Greenspun, Barbara & Hank JHS	Greenspun JHS
2325		Swainston, Theron L MS	Swainston MS
2326		White, Thurman Academy of the Arts MS	White MS
2327		Becker, Ernest MS	Becker MS
2328		Sawyer, Grant MS	Sawyer MS
2329		Lyon, Mack MS	Lyon MS
2330	290228	West, Dr. Charles I. Preparatory Academy	West Prep J-SHS
2331		Lied STEM Academy MS	Lied STEM ACAD MS
2332		Keller, Duane D MS	Keller MS
2333		Molasky, Irwin & Susan JHS	Molasky JHS
2334		Silvestri, Charles JHS	Silvestri JHS
2335		Cortney, Francis H JHS	Cortney JHS
2336		Indian Springs MS	Indian Springs MS
2337		Lawrence, Clifford J JHS	Lawrence JHS
2338		Miller, Bob MS	Miller MS
2339		Rogich, Sig MS	Rogich MS
2341		Leavitt, Justice Myron E MS	Leavitt MS
2342		Cram, Brian & Teri MS	Cram MS

2343		Monaco, Mario C & JoAnne MS	Monaco MS
2344		Schofield, Jack Lund MS	Schofield MS
2345		Sedway, Marvin M MS	Sedway MS
2346		Harney, Kathleen & Tim MS	Harney MS
2347		Fertitta, Victoria MS	Fertitta MS
2348		Cadwallader, Ralph MS	Cadwallader MS
2349		Canarelli, Lawrence & Heidi MS	Canarelli MS
2350		Hughes, Charles Arthur MS	Hughes MS
2352		Findlay, Clifford O MS	Findlay MS
2353		Mannion, Jack & Terry MS	Mannion MS
2354		Saville, Anthony MS	Saville MS
2355		Webb, Del E MS	Webb MS
2356		Mack, Jerome MS	Mack MS
2357		Bailey, Dr William H MS	Bailey MS
2359		Johnston, Carroll M STEM Academy of Env Studies	Johnston MS
2360		Tarkanian, Lois & Jerry MS	Tarkanian MS
2361		Escobedo, Edmundo Eddie Sr MS	Escobedo MS
2362		Faiss, Wilbur & Theresa MS	Faiss MS
2368		Gunderson, Barry and June MS	Gunderson MS
2369		Mackey, Jo MS	Mackey MS
2401	290097	Clark, Ed W HS	Clark HS
2402	290100	Las Vegas HS	Las Vegas HS
2403	290103	Rancho HS	Rancho HS
2404	290102	Valley HS	Valley HS
2405	290104	Western HS	Western HS
2406	290090	Basic Academy of Int'l Studies HS	Basic ACAD HS
2408	290088	Morris Sunset HS	Morris Sunset HS
2409	290096	Chaparral HS	Chaparral HS
2410	290098	Eldorado HS	Eldorado HS
2411	290091	Bonanza HS	Bonanza HS
2412	290101	Southeast Career Technical Academy HS	SECTA HS
2414	290115	Cimarron-Memorial HS	Cimarron Mem HS
2415	290121	Cheyenne HS	Cheyenne HS
2416	290084	Green Valley HS	Green Valley HS
2417	290118	Durango HS	Durango HS

2418	290119	Las Vegas Academy of the Arts HS	Las Vegas ACAD HS
2420	290134	Advanced Technologies Academy HS	Adv Tech ACAD HS
2421	290132	Silverado HS	Silverado HS
2422	290087	College of So NV HS East	CSN East HS
2423	290082	College of So NV HS West	CSN West HS
2424	290220	Mojave HS	Mojave HS
2425	290200	Palo Verde HS	Palo Verde HS
2426	290081	College of So NV HS South	CSN South HS
2427	290209	Shadow Ridge HS	Shadow Ridge HS
2428	290197	Liberty HS	Liberty HS
2429	290194	Canyon Springs HS	Canyon Springs
2430	290198	Del Sol Academy of Performing Arts HS	Del Sol ACAD HS
2431	290202	Spring Valley HS	Spring Valley
2432	290215	Veterans Tribute CTA HS	VTCTA HS
2433	290213	Southwest Career & Technical Academy HS	SWCTA HS
2434	290210	Sunrise Mountain HS	Sunrise Mountain HS
2435	290244	West Career & Technical Academy HS	WCTA HS
2501		Brown, Hannah Marie ES	Brown H M ES
2601	290020	Boulder City HS	Boulder City HS
2602	290125	Moapa Valley HS	Moapa Valley HS
2603	290025	Virgin Valley HS	Virgin Valley HS
2604	290093	Indian Springs HS	Indian Springs HS
2607	290191	Centennial HS	Centennial HS
2608	290073	Foothill HS	Foothill HS
2609	290192	Desert Pines HS	Desert Pines HS
2611	290179	Sierra Vista HS	Sierra Vista HS
2612	290069	Coronado HS	Coronado HS
2618	290204	Arbor View HS	Arbor View HS
2619	290223	Legacy HS	Legacy HS
2620	290225	Northwest Career-Technical Academy HS	NWCTA HS
2623	290219	Desert Oasis HS	Desert Oasis HS
2624	290227	East Career and Technical Academy HS	ECTA HS
2625	290203	NV Learning Academy J-SHS	NV LRN Academy
2626		NV Learning Academy ES	NV LRN ACAD ES
2627	290026	Central Technical Training Academy	CTTA

2628	031789	Northeast Career and Technical Academy HS	NECTA HS
2716	977015	Acceleration Academy	Acceleration Academy
2777	991854	Clark County Detention Ctr J-SHS	CC Detention JSHS
2901		Northeast Career and Technical Academy PK	NECTA PK
2902	225633	South Career and Technical Academy HS	SCTA HS
2903		Cheyenne PK	Cheyenne PK
2904		Cimarron-Memorial PK	Cimarron Mem PK
2905		Desert Pines PK	Desert Pines PK
2906		Western PK	Western PK
2907		Bonanza PK	Bonanza PK
2910	991929	Stewart, Helen J	Stewart
2911	991741	Variety J-SHS	Variety JSHS
2912	290163	Juvenile Detention 6-12 J-SHS	Juvenile Court
2913	991733	Spring Mountain J-SHS	Spring Mtn JSHS
2916	991728	Miley Achievement Ctr J-SHS	Miley Achvmt SEC
2917		Miley Achievement Center ES	Miley Achvmt ES
2919	991874	Summit View Youth J-SHS	Summit View JSHS
2922	290186	Burk Horizon-Southwest Sunset HS	Burk Horizon SW HS
2923	290129	Global Community HS	Global Community HS
2924	290133	Cowan Sunset Southeast HS	Cowan Sunset SE
2926		Desert Willow ES	Desert Willow ES
2927	991742	Desert Willow J-SHS	Desert Willow JSHS
2928	290237	South Academic Center J-SHS	South Cont JSHS
2932	991716	Cowan Academic Center J-SHS	Cowan Behavior
2933	290201	Peterson Academic Center J-SHS	Peterson Behavior
2935		Variety ES	Variety ES
2936		Child Haven K-12	Child Haven
2939		Juvenile Detention 3-5 ES	Juvenile Det ES
2940	991933	High Desert State Prison Adult HS	Prison Program
2941	290113	Adult Education Programs	Adult Ed
2953		So Desert Correctional Center Adult	SDCC
2954		McClure, Florence Women's Corr	McClure Corr Ctr
2955	290214	Desert Rose HS	Desert Rose ALT
2956	976280	High Desert State Prison YOP	HGHDSRTYOP
2957	290013	Mission High School	Mission HS

2958	820907	Amy Ayoub Academy of Hope	Amy Ayoub Academy of Hope
2960		Child Find	Clark Child Find
2965	290245	Quest Program	Quest Program
3201		Gardnerville Elementary School	Gardnerville ES
3202		Zephyr Cove Elementary School	Zephyr Cove ES
3206		Jacks Valley Elementary School	Jacks Valley ES
3207		G. L. Scarselli Elementary School	Scarselli ES
3209		Pinon Hills Elementary School	Pinon Hills ES
3210		Minden Elementary School	Minden ES
3301		Carson Valley Middle School	Carson Valley MS
3302		Pau Wa Lu Middle School	Pau Wa Lu MS
3501	290075	Douglas High School	Douglas HS
3502	290190	George Whittell High School	Whittell HS
3503	991731	Jacobsen High School	Jacobsen HS
3504	290239	ASPIRE Academy High School	ASPIRE HS
3601	977018	Douglas Nevada Online	Douglas Online
3901	991730	ALT School	Douglas Alternative
3903		Douglas County Adult School	Douglas Adult Ed
3950		Child Find	Douglas Child Find
4104		Independence Valley Elementary School	Independence Vly ES
4105		Jackpot Elementary School	Jackpot ES
4107		Montello Elementary School	Montello ES
4108		Mound Valley Elementary School	Mound Valley ES
4111		Ruby Valley Elementary School	Ruby Valley ES
4120		Liberty Peak Elementary School	Liberty Peak ES
4202		Grammar School 2	Elko Grammar ES
4203		Northside Elementary School	Northside ES
4204		Southside Elementary School	Southside ES
4205		Carlin Elementary School	Carlin ES
4206		Owyhee Elementary School	Owyhee ES
4207		Wells Elementary School	Wells ES
4208		West Wendover Elementary School	W Wendover ES
4209		Mountain View Elementary School	Mtn View ES
4210		Spring Creek Elementary School	Spring Creek ES
4211		Sage Elementary School	Sage ES

4213		Flagview Intermediate School	Flagview Intermediate
4501		Carlin Jr High School	Carlin JHS
4502		Wells Jr High School	Wells JHS
4503		Adobe Middle School	Adobe MS
4504		Spring Creek Middle School	Spring Creek MS
4505		Jackpot Jr High School	Jackpot JHS
4506		Owyhee Jr High School	Owyhee JHS
4507		West Wendover Middle School	W Wendover MS
4601	290030	Carlin High School	Carlin HS
4602	290175	Wells High School	Wells HS HS
4603	290045	Elko High School	Elko HS
4604	290130	Owyhee High School	Owyhee HS
4605	290086	Jackpot High School	Jackpot HS
4606	290049	Spring Creek High School	Spring Creek HS
4607	290178	West Wendover High School	W Wendover HS
4610	290022	Northeastern Nevada Virtual Academy	NE NV Virtual
4902		Adult Education	Elko Adult Ed
4904		Early Childhood	Early Childhood
4905		Early Childhood GBC	Early Childhood GBC
4908	977436	Battle Born Youth Challenge Academy	Battle Born Academy
5101		Dyer Elementary School	Dyer ES
5102		Goldfield Elementary School	Goldfield ES
5501	977099	Esmeralda Virtual High School	Esmeralda Virtual HS
6101		Crescent Valley Elementary	Crescent Valley ES
6103		Eureka Elementary School	Eureka ES
6601	290055	Eureka County High School	Eureka HS
7101		Denio	Denio ES
7103		Kings River	Kings River ES
7104		Orovada School	Orovada ES
7105		Paradise Valley School	Paradise Valley ES
7106		French Ford Elementary School	French Ford ES
7201		Sonoma Heights Elementary	Sonoma Heights ES
7203		McDermitt Elementary	McDermitt ES
7205		Grass Valley Elementary	Grass Valley ES
7301		Winnemucca Junior High School	Winnemucca JHS

7302		McDermitt Junior High School	McDermitt JHS
7501	290180	Albert M. Lowry High School	Lowry HS
7601	290112	McDermitt High School	McDermitt HS
7903		Humboldt Adult Education Program	Humboldt Adult Ed
7930		Child Find	Humboldt Child Find
8201		Battle Mountain Elementary School	Battle Mtn ES
8302		Eleanor Lemaire Junior High School	Lemaire JHS
8601	290010	Battle Mountain High School	Battle Mtn HS
8602	290005	Austin Combined Schools	Austin Combined
8902		Lander County Adult Ed	Lander Adult Ed
9102		Pahranagat Valley Elementary School	Pahranagat Valley ES
9201		Caliente Elementary School	Caliente ES
9202		Panaca Elementary School	Panaca ES
9203		Pioche Elementary School	Pioche ES
9301		Meadow Valley Middle School	Meadow Valley MS
9302		Pahranagat Valley Middle School	Pahranagat Valley MS
9501	290135	Lincoln County High School	Lincoln HS
9601	290000	Pahranagat Valley High School	Pahranagat Valley HS
9602	290028	C O Bastian High School	C O Bastian
9603		Lincoln County Adult High School	Lincoln Ad Ed HS
9903		Lincoln County Adult Corrections	Lincoln Adult Ed CO
10201		Dayton Elementary School	Dayton ES
10202		Yerington Elementary School	Yerington ES
10203		Fernley Elementary School	Fernley ES
10205		Silver Stage Elementary School	Silver Stage ES
10206		East Valley Elementary School	East Valley ES
10208		Dayton Intermediate School	Dayton Intermediate
10209		Cottonwood Elementary School	Cottonwood ES
10210		Sutro Elementary School	Sutro ES
10211		Riverview Elementary School	Riverview ES
10302		Yerington Intermediate School	Yerington Intermediate
10303		Fernley Intermediate School	Fernley Intermediate
10304		Silver Stage Middle School	Silver Stage MS
10305		Silverland Middle School	Silverland MS
10601	290065	Fernley High School	Fernley HS

10602	290150	Smith Valley Schools	Smith Valley Combined
10603	290185	Yerington High School	Yerington HS
10604	290041	Dayton High School	Dayton HS
10605	290251	Silver Stage High School	Silver Stage HS
10902	991739	Eagle Ridge High School	Eagle Ridge HS
10907		Lyon County Adult Education	Lyon Adult Ed
10950		Child Find	Lyon Child Find
10960		LyOnline	LyOnline
11201		Hawthorne Elementary	Hawthorne ES
11202		Schurz Elementary	Schurz ES
11203		Hawthorne Junior High	Hawthorne JHS
11601	290085	Mineral County High School	Mineral HS
11925		Mineral County Adult Education	Mineral Adult Ed
12102		Manse Elementary School	Manse ES
12103		Round Mountain Elementary School	Round Mtn ES
12105		Gabbs Elementary School	Gabbs ES
12106		Amargosa Valley Elementary School	Amargosa Valley ES
12108		J G Johnson Elementary School	JG Johnson ES
12201		Beatty Elementary School	Beatty ES
12202		Tonopah Elementary School	Tonopah ES
12206		Mt Charleston Elementary School	Charleston ES
12207		Hafen Elementary School	Hafen ES
12210		Floyd Elementary School	Floyd ES
12301		Rosemary Clarke Middle School	Rosemary Clarke MS
12311		Beatty Middle School	Beatty MS
12312		Tonopah Middle School	Tonopah MS
12313		Round Mountain Middle School	Round Mtn MS
12315		Gabbs Middle School	Gabbs MS
12316		Amargosa Valley Middle School	Amargosa Valley MS
12601	290015	Beatty High School	Beatty HS
12602	290070	Gabbs High School	Gabbs HS
12603	290165	Tonopah High School	Tonopah HS
12604	290137	Pahrump Valley High School	Pahrump Valley HS
12605	290139	Round Mountain High School	Round Mtn HS
12606	292224	Pathways High School	Pathways HS

12607		Pathways Middle School	Pathways MS
12609		Pathways Elementary School	Pathways ES
12902	977021	NCSD Adult Education	Nye Adult Ed
13201		Bordewich/Bray Elementary	Bordewich Bray ES
13202	977016	Carson Adult High School	Carson Adult ED
13203		Edith W. Fritsch Elementary	Fritsch ES
13204		Fremont Elementary	Fremont ES
13207		Al Seeliger Elementary	Seeliger ES
13209		Empire Elementary	Empire ES
13211		Mark Twain Elementary	Mark Twain ES
13212		Carson Montessori	Carson Montessori
13301		Carson Middle School	Carson MS
13302		Eagle Valley Middle School	Eagle Valley MS
13501	290035	Carson High School	Carson HS
14101		Imlay Elementary School	Imlay ES
14201		Lovelock Elementary School	Lovelock ES
14301		Pershing County Middle School	Pershing MS
14601	290105	Pershing County High School	Pershing HS
14903		Pershing Adult High School	Pershing Adult Ed
14991		Coal Canyon High School	Coal Canyon HS
15101		Hugh Gallagher Elementary School	Gallagher ES
15102		Hillside Elementary School	Hillside ES
15301		Virginia City Middle School	Virginia City MS
15601	290170	Virginia City High School	Virginia City HS
16201		ANDERSON ELEMENTARY	Anderson ES
16202		ECHO LODER ELEMENTARY SCHOOL	Loder ES
16203		ELMCREST ELEMENTARY	Elmcrest ES
16204		GLENN DUNCAN S.T.E.M. ACADEMY	Duncan ES
16205		GRACE WARNER ELEMENTARY	Warner ES
16206		HUNTER LAKE ELEMENTARY	Hunter Lake ES
16207		JESSIE BECK ELEMENTARY	Beck ES
16208		LIBBY BOOTH ELEMENTARY	Booth ES
16209		MAMIE TOWLES ELEMENTARY	Towles ES
16210		ROLLAN MELTON ELEMENTARY	Melton ES
16211		MOUNT ROSE K-8 ACADEMY OF LANGUAGES	Mount Rose K 8

16212		DOUBLE DIAMOND ELEMENTARY	Double Diamond ES
16213		PEAVINE ELEMENTARY	Peavine ES
16214		RITA CANNAN ELEMENTARY	Cannan ES
16215		ROGER CORBETT ELEMENTARY	Corbett ES
16216		ROY GOMM ELEMENTARY	Gomm ES
16218		SMITHRIDGE S.T.E.M. ACADEMY	Smithridge ES
16219		STEAD ELEMENTARY	Stead ES
16220		VETERANS MEMORIAL S.T.E.M. ACADEMY	Veterans Memorial STEM
16221		AGNES RISLEY ELEMENTARY	Risley ES
16222		ALICE MAXWELL ELEMENTARY	Maxwell ES
16223		FLORENCE DRAKE ELEMENTARY	Drake ES
16224		GREENBRAE ELEMENTARY	Greenbrae ES
16225		KATE SMITH ELEMENTARY	Smith Kate ES
16226		LENA JUNIPER ELEMENTARY	Juniper ES
16227		LINCOLN PARK ELEMENTARY	Lincoln Park ES
16228		ROBERT MITCHELL ELEMENTARY	Mitchell ES
16229		BROWN ELEMENTARY	Brown ES
16230		HUFFAKER ELEMENTARY	Huffaker ES
16231		DOROTHY LEMELSON S.T.E.M. ACADEMY ES	Lemelson STEM ES
16232		LEMMON VALLEY ELEMENTARY	Lemmon Valley ES
16233		PLEASANT VALLEY ELEMENTARY	Pleasant Valley ES
16234		SUN VALLEY ELEMENTARY	Sun Valley ES
16235		VERDI ELEMENTARY	Verdi ES
16237		NATCHEZ ELEMENTARY	Natchez ES
16238		LLOYD DIEDRICHSEN ELEMENTARY	Diedrichsen ES
16239		KATHERINE DUNN ELEMENTARY	Dunn ES
16240		VIRGINIA PALMER ELEMENTARY	Palmer ES
16241		JESSE HALL ELEMENTARY SCHOOL	Hall ES
16242		MIGUEL SEPULVEDA ELEMENTARY SCHOOL	Sepulveda ES
16243		NICK POULAKIDAS ELEMENTARY SCHOOL	Poulakidas ES
16244		JOHN BOHACH ELEMENTARY SCHOOL	JOHN BOHACH ES
16245		MICHAEL INSKEEP ELEMENTARY SCHOOL	Inskeep ES
16246		JWOOD RAW ELEMENTARY SCHOOL	Raw ES
16251		INCLINE ELEMENTARY	Incline ES
16256		NANCY GOMES ELEMENTARY	Gomes ES

16257		ELIZABETH LENZ ELEMENTARY	Lenz ES
16258		EDWIN S. DODSON ELEMENTARY	Dodson ES
16259		JERRY WHITEHEAD ELEMENTARY	Whitehead ES
16260		ALICE SMITH ELEMENTARY	Smith Alice ES
16261		CAUGHLIN RANCH ELEMENTARY	Caughlin Ranch ES
16262		HIDDEN VALLEY ELEMENTARY	Hidden Valley ES
16263		SILVER LAKE ELEMENTARY	Silver Lake ES
16264		GEORGE WESTERGARD ELEMENTARY	Westergard ES
16265		ALYCE TAYLOR ELEMENTARY	Taylor ES
16266		LOIS ALLEN ELEMENTARY	Allen ES
16267		MARVIN MOSS ELEMENTARY	Moss ES
16268		DESERT HEIGHTS ELEMENTARY	Desert Heights ES
16269		SPANISH SPRINGS ELEMENTARY	Spanish Spgs ES
16270		SARAH WINNEMUCCA ELEMENTARY	Winnemucca ES
16271		BUD BEASLEY ELEMENTARY	Beasley ES
16272		DONNER SPRINGS ELEMENTARY	Donner Springs ES
16273		BERNICE MATHEWS ELEMENTARY	Mathews ES
16274		TED HUNSBERGER ELEMENTARY	Hunsberger ES
16275		ESTHER BENNETT ELEMENTARY	Bennett ES
16276		VAN GORDER ELEMENTARY	Van Gorder ES
16278		Bailey Charter School	Bailey CH ES
16279		Coral Academy Elementary-South	Coral Acad ES-South
16280		Coral Academy Elementary-Northwest	Coral Acad ES-Northwest
16281		Mariposa Language and Learning Academy	Mariposa CS
16282		High Desert Montessori	High Desert CS
16301		ARCHIE CLAYTON PRE-A.P. ACADEMY	Clayton Academy
16303		DARREL SWOPE MIDDLE SCHOOL	Swope MS
16304		E. OTIS VAUGHN MIDDLE SCHOOL	Vaughn MS
16305		FRED W. TRANER MIDDLE SCHOOL	Traner MS
16306		GEORGE L. DILWORTH S.T.E.M ACADEMY	Dilworth MS
16307		SPARKS MIDDLE SCHOOL	Sparks MS
16308		WILLIAM OBRIEN MIDDLE SCHOOL	OBrien MS
16309		INCLINE MIDDLE SCHOOL	Incline MS
16310		BILLINGHURST MIDDLE SCHOOL	Billinghurst MS
16311		LOU MENDIVE MIDDLE SCHOOL	Mendive MS

16312	290249	Coral Academy High School	Coral Acad HS
16315		KENDYL DEPOALI MIDDLE SCHOOL	Depoali MS
16316		YVONNE SHAW MIDDLE SCHOOL	Shaw MS
16317		COLD SPRINGS MIDDLE SCHOOL	Cold Springs MS
16318		Coral Academy Elementary	Coral Acad ES
16319		SKY RANCH MIDDLE SCHOOL	Sky Ranch MS
16320		Coral Academy Middle School	Coral Academy MS
16321		DESERT SKIES MIDDLE SCHOOL	Desert Skies MS
16322		MARCE HERZ MIDDLE SCHOOL	Herz MS
16501	290142	EARL WOOSTER HIGH SCHOOL	Wooster HS
16502	290145	RENO HIGH SCHOOL	Reno HS
16503	290155	SPARKS HIGH SCHOOL	Sparks HS
16504	290144	PROCTER R. HUG HIGH SCHOOL	Hug HS
16505	290141	EDWARD C. REED HIGH SCHOOL	Reed HS
16507	290272	WASHOE INSPIRE ACADEMY	Inspire Academy
16508	290143	ROBERT MCQUEEN HIGH SCHOOL	McQueen HS
16509	290149	GALENA HIGH SCHOOL	Galena HS
16510	290138	INNOVATIONS HIGH SCHOOL	Innovations HS
16511	018289	DEBBIE SMITH CTE ACADEMY	Debbie Smith CTE
16601	290080	GERLACH K-12 SCHOOL	Gerlach K 12
16602	290092	INCLINE HIGH SCHOOL	Incline HS
16603	290157	TMCC MAGNET SCHOOL	TMCC Magnet
16605	997622	Sierra Nevada Academy Charter	Sierra NV Acad CS
16606	290270	SPANISH SPRINGS HIGH SCHOOL	Spanish Springs HS
16607	290177	NORTH VALLEYS HIGH SCHOOL	North Valleys HS
16608	290260	Academy For Career Education	ACE ACAD
16609	290187	DAMONTE RANCH HIGH SCHOOL	Damonte Ranch HS
16610	290248	enCompass Academy	enCompass CS
16611	290247	ACADEMY OF ARTS CAREERS & TECH	Arts Careers Tech
16900		EARLY CHILDHOOD EDUCATION	Washoe Early Childhood
16904		COLD SPRINGS EARLY CHILDHOOD CENTER	Cold Springs ECC
16911		MARVIN PICOLLO ELEMENTARY	Picollo K 12
16917	290232	TURNING POINT	Turning Point
16921		RISE ACADEMY FOR ADULT ACHIEVEMENT	Rise Adult Achievement
16922		TRANSITION ACADEMY	TRANSITION ACADEMY

16923	290242	NORTH STAR ONLINE SCHOOL	North Star Online
16930		CHILD FIND	WASHOE CHILD FIND
17101		Lund Elementary	Lund ES
17103		Baker Elementary	Baker ES
17201		David E Norman Elementary	Norman ES
17203		McGill Elementary	McGill ES
17204		Early Childhood	WP Early Childhood
17301		White Pine Middle School	White Pine MS
17502	290050	White Pine High School	White Pine HS
17601	290110	Lund High School	Lund JSHS
17903	991738	Steptoe Valley High School	Steptoe Valley HS
17904		Steptoe Valley Adult High School	Steptoe Valley Adult Ed
17930		Child Find	WP Child Find
17999		Home School	WP Home School
38435		Freedom Classical Academy K-8	Freedom Class ACAD
39438		Legacy Traditional School North Valley	Legacy N Valley
39439		Legacy Traditional School Cadence	Legacy Cadence
39440		Legacy Traditional School Southwest Las Vegas	Legacy SW
43100		Futuro Academy Elementary	Futuro ACAD
44437		Mater Academy of Northern Nevada	Mater Northern NV
45100		FFN	FFN
45101		CSA	CSA
45102		Licensed Child Care Centers	Licensed Child Care
45105		Acelero Learning Clark County	Acelero Learning
45111		CSN ECE Lab	CSN Lab
45115		Kids R Kids	Kids R Kids
45123		Sunrise Childrens Foundation	Sunrise Foundation
45124		YMCA	YMCA
45125		Boys and Girls Club	BGC
45126		United Way of Northern Nevada and the Sierra	UWNNS
45127		United Way of Southern Nevada	UWSN
45128		University of Nevada Las Vegas	UNLV
45500		CLV Strong Start GO	CLV Strong
46400	290011	DPAC Nevada	DPAC Nevada
47434	290007	Sports Leadership and Management Academy	SLAM

48433	290235	Equipo Academy	Equipo ACAD
49100		Mater Cactus Park	Mater Cactus Park
49200		Mater Sahara	Mater Sahara
49432		Mater Mountain Vista	Mater Mtn Vista
49433		Mater Bonanza	Mater Bonanza
49434	290019	Mater East	Mater East
50431	290006	Amplus Durango	Amplus Durango
50432		Amplus Rainbow	Amplus Rainbow
51430	290233	Founders Academy of Las Vegas	Founders ACAD
52429	290016	Leadership Academy of Nevada	Leadership ACAD
54428		Learning Bridge	Learning Bridge
55200		Doral Academy Cactus	Doral Cactus
55201		Doral Academy Fire Mesa	Doral Fire Mesa
55202	290009	Doral Academy Red Rock	Doral Red Rock
55203		Doral Academy Saddle	Doral Saddle
55204		Doral Academy West Pebble	Doral W Pebble
57424		Honors Academy of Literature	Honors ACAD
58422		Pinecrest Academy of Nevada Horizon	Pinecrest Horizon
58423	290002	Pinecrest Academy of Nevada Cadence	Pinecrest Cadence
58425		Pinecrest Academy of Nevada Inspirada	Pinecrest Inspirada
58427		Pinecrest Academy of Nevada St Rose	Pinecrest St Rose
58428	290236	Pinecrest Academy of Nevada Sloan Canyon	Pinecrest Sloan
58429	292204	Pinecrest Academy of Nevada Virtual	Pinecrest Virtual
58430		Pinecrest Academy of Nevada Springs	Pinecrest Springs
59119		Somerset Academy North Las Vegas	Somerset NLV
59120	290234	Somerset Academy Losee	Somerset Losee
59121		Somerset Academy Lone Mountain	Somerset Lone Mtn
59122	290230	Somerset Academy Sky Pointe	Somerset Sky Pointe
59123		Somerset Academy Stephanie	Somerset Stephanie
59124		Somerset Academy Aliante	Somerset Aliante
59125		Somerset Academy Skye Canyon	Somerset Skye Canyon
60401	290199	Explore Knowledge Academy	Explore Knowledge Acad
61415		Discovery Preparatory Academy Sandhill	Discovery Sandhill
61417		Discovery Preparatory Academy Hillpointe	Discovery Hillpointe
62101		Do & Be Arts Academy of Excellence	Do & Be Arts Acad

64087		Rainbow Dreams Early Learning Academy	Rainbow Dreams Acad
65414	290003	Oasis Academy	Oasis ACAD
66436		Doral Academy of Northern Nevada	Doral Northern NV
67201	290217	The Delta Academy	Delta Acad
68410		Elko Institute for Academic Achievement	Elko Institute
69101		Innovations International Charter School Oakey	Innovations Oakey
69201	290218	Innovations International Charter School Sahara	Innovations Sahara
72416		Quest Academy Northwest	Quest Northwest
74418		Imagine School Mountain View	Imagine Mtn View
75401		FuturEdge Academy	FuturEdge Acad
76412	290265	Alpine Academy High School	Alpine Acad HS
77401	290188	Odyssey Charter School	Odyssey
78411		Silver Sands Montessori	Silver Sands
79903	290047	Independence High School	Independence HS
81101	976275	Nevada State High School Downtown	NSHS Downtown
81102	976277	Nevada State High School Summerlin	NSHS Summerlin
81103	290067	Nevada State High School Henderson	NSHS Henderson
81104	976525	Nevada State High School Sunrise	NSHS Sunrise
81106	976829	Nevada State High School Southwest	NSHS SW
81107	977022	Nevada State High School Downtown Henderson	NSHS DownTwn Hend
81108	977023	Nevada State High School Northwest	NSHS NW
81109	977619	Nevada State High School North Las Vegas	NSHS North Las Vegas
84406	290207	Davidson Academy	Davidson Acad
85405	290240	Nevada Connections Academy	NV Connections ACAD
86404	290243	Nevada Virtual Charter School	Nevada Virtual
87310		Coral Academy Centennial Hills	CASLV Centennial
87311		Coral Academy Nellis AFB	CASLV Nellis AFB
87312	290216	Coral Academy Sandy Ridge	CASLV Sandy Ridge
87313		Coral Academy Tamarus	CASLV Tamarus
87314		Coral Academy Windmill	CASLV Windmill
87315		Coral Academy Eastgate	CASLV Eastgate
87316	848486	Coral Academy Cadence	CASLV Cadence
89409	290226	Beacon Academy of Nevada	Beacon ACAD
92201		WYLEES	WYLEES
95301	753136	Southern Nevada Trades High School	Southern NV Trades HS

96601	629829	Thrive Point Academy	Thrive Point Acad
97101		Vegas Vista Academy	Vegas Vista Acad
98101		Nevada Classical Academy Elko	Nevada Classical Academy Elko
101101		NV Rise Academy Charter School	NV Rise CS
104101	976524	Nevada State High School II Meadowwood	NSHS II Meadowwood
105101		Signature Preparatory	Signature Prep CS
106101		Pinecrest Academy of Northern Nevada	Pinecrest Northern NV
107101	290024	Explore Academy	Explore ACAD
110100	916951	CIVICA Academy	CIVICA Acad
113100		Young Womens Leadership Academy of Las Vegas	YWLA
115100		Strong Start Academy	Strong Start Academy
127100		Academies of Math and Science Nellis	AMS Nellis
300100		Kesher Academy	Kesher Academy

School Type	Charter Status	Grade Levels Offered - Low Grade	Grade Levels Offered - High Grade
EL: Early Learning	NO: N/A	PK: Pre K	PK: Pre K
RG: Regular	NO: N/A	02: Second Grade	03: Third Grade
RG: Regular	NO: N/A	KG: Kindergarten	01: First Grade
RG: Regular	NO: N/A	04: Fourth Grade	05: Fifth Grade
RG: Regular	NO: N/A	06: Sixth Grade	08: Eighth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
AD: Adult	NO: N/A	AD: Adult	AD: Adult
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	KG: Kindergarten	KG: Kindergarten
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
EL: Early Learning	NO: N/A	PK: Pre K	PK: Pre K

[illegible]

[illegible]

[illegible]

RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
SE: Special Education	NO: N/A	PK: Pre K	12: Twelfth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
SE: Special Education	NO: N/A	PK: Pre K	KG: Kindergarten
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade

[illegible]

[illegible]

[illegible]

[illegible]

RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
CTE: Career and Technical	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	11: Eleventh Grade	12: Twelfth Grade
RG: Regular	NO: N/A	11: Eleventh Grade	12: Twelfth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	11: Eleventh Grade	12: Twelfth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
CTE: Career and Technical	NO: N/A	09: Ninth Grade	12: Twelfth Grade
CTE: Career and Technical	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
CTE: Career and Technical	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
CTE: Career and Technical	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
CTE: Career and Technical	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	06: Sixth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
CTE: Career and Technical	NO: N/A	09: Ninth Grade	12: Twelfth Grade

CTE: Career and Technical	NO: N/A	09: Ninth Grade	12: Twelfth Grade
AL: Alternative	NO: N/A	09: Ninth Grade	12: Twelfth Grade
JVC: Juvenile Correctional	NO: N/A	06: Sixth Grade	12: Twelfth Grade
EL: Early Learning	NO: N/A	PK: Pre K	PK: Pre K
CTE: Career and Technical	NO: N/A	09: Ninth Grade	12: Twelfth Grade
EL: Early Learning	NO: N/A	PK: Pre K	PK: Pre K
EL: Early Learning	NO: N/A	PK: Pre K	PK: Pre K
EL: Early Learning	NO: N/A	PK: Pre K	PK: Pre K
EL: Early Learning	NO: N/A	PK: Pre K	PK: Pre K
EL: Early Learning	NO: N/A	PK: Pre K	PK: Pre K
SE: Special Education	NO: N/A	PK: Pre K	12: Twelfth Grade
SE: Special Education	NO: N/A	06: Sixth Grade	12: Twelfth Grade
JVC: Juvenile Correctional	NO: N/A	06: Sixth Grade	12: Twelfth Grade
JVC: Juvenile Correctional	NO: N/A	06: Sixth Grade	12: Twelfth Grade
SE: Special Education	NO: N/A	06: Sixth Grade	12: Twelfth Grade
SE: Special Education	NO: N/A	PK: Pre K	05: Fifth Grade
JVC: Juvenile Correctional	NO: N/A	06: Sixth Grade	12: Twelfth Grade
AL: Alternative	NO: N/A	09: Ninth Grade	12: Twelfth Grade
AL: Alternative	NO: N/A	09: Ninth Grade	12: Twelfth Grade
AL: Alternative	NO: N/A	09: Ninth Grade	12: Twelfth Grade
SE: Special Education	NO: N/A	PK: Pre K	05: Fifth Grade
SE: Special Education	NO: N/A	06: Sixth Grade	12: Twelfth Grade
AL: Alternative	NO: N/A	06: Sixth Grade	12: Twelfth Grade
AL: Alternative	NO: N/A	06: Sixth Grade	12: Twelfth Grade
AL: Alternative	NO: N/A	06: Sixth Grade	12: Twelfth Grade
SE: Special Education	NO: N/A	PK: Pre K	05: Fifth Grade
RP: Reportable Program	NO: N/A	KG: Kindergarten	12: Twelfth Grade
JVC: Juvenile Correctional	NO: N/A	03: Third Grade	05: Fifth Grade
CO: Correctional	NO: N/A	AD: Adult	AD: Adult
AD: Adult	NO: N/A	AD: Adult	AD: Adult
CO: Correctional	NO: N/A	AD: Adult	AD: Adult
CO: Correctional	NO: N/A	AD: Adult	AD: Adult
AL: Alternative	NO: N/A	09: Ninth Grade	12: Twelfth Grade
JVC: Juvenile Correctional	NO: N/A	09: Ninth Grade	12: Twelfth Grade
AL: Alternative	NO: N/A	06: Sixth Grade	12: Twelfth Grade

AL: Alternative	NO: N/A	06: Sixth Grade	12: Twelfth Grade
RP: Reportable Program	NO: N/A	PK: Pre K	12: Twelfth Grade
AL: Alternative	NO: N/A	KG: Kindergarten	12: Twelfth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	06: Sixth Grade	08: Eighth Grade
RG: Regular	NO: N/A	06: Sixth Grade	08: Eighth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	06: Sixth Grade	12: Twelfth Grade
JVC: Juvenile Correctional	NO: N/A	07: Seventh Grade	12: Twelfth Grade
AL: Alternative	NO: N/A	07: Seventh Grade	12: Twelfth Grade
AL: Alternative	NO: N/A	06: Sixth Grade	08: Eighth Grade
AL: Alternative	NO: N/A	04: Fourth Grade	12: Twelfth Grade
AD: Adult	NO: N/A	AD: Adult	AD: Adult
RP: Reportable Program	NO: N/A	PK: Pre K	12: Twelfth Grade
RG: Regular	NO: N/A	KG: Kindergarten	08: Eighth Grade
RG: Regular	NO: N/A	KG: Kindergarten	06: Sixth Grade
RG: Regular	NO: N/A	KG: Kindergarten	08: Eighth Grade
RG: Regular	NO: N/A	KG: Kindergarten	08: Eighth Grade
RG: Regular	NO: N/A	KG: Kindergarten	08: Eighth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	KG: Kindergarten	06: Sixth Grade
RG: Regular	NO: N/A	PK: Pre K	06: Sixth Grade
RG: Regular	NO: N/A	KG: Kindergarten	06: Sixth Grade
RG: Regular	NO: N/A	PK: Pre K	08: Eighth Grade
RG: Regular	NO: N/A	KG: Kindergarten	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade

RG: Regular	NO: N/A	06: Sixth Grade	06: Sixth Grade
RG: Regular	NO: N/A	07: Seventh Grade	08: Eighth Grade
RG: Regular	NO: N/A	07: Seventh Grade	08: Eighth Grade
RG: Regular	NO: N/A	07: Seventh Grade	08: Eighth Grade
RG: Regular	NO: N/A	06: Sixth Grade	08: Eighth Grade
RG: Regular	NO: N/A	07: Seventh Grade	08: Eighth Grade
RG: Regular	NO: N/A	07: Seventh Grade	08: Eighth Grade
RG: Regular	NO: N/A	06: Sixth Grade	08: Eighth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	KG: Kindergarten	12: Twelfth Grade
AD: Adult	NO: N/A	AD: Adult	AD: Adult
EL: Early Learning	NO: N/A	PK: Pre K	PK: Pre K
SE: Special Education	NO: N/A	PK: Pre K	KG: Kindergarten
AL: Alternative	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	PK: Pre K	08: Eighth Grade
RG: Regular	NO: N/A	PK: Pre K	08: Eighth Grade
AL: Alternative	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	PK: Pre K	06: Sixth Grade
RG: Regular	NO: N/A	PK: Pre K	06: Sixth Grade
RG: Regular	NO: N/A	07: Seventh Grade	12: Twelfth Grade
RG: Regular	NO: N/A	PK: Pre K	08: Eighth Grade
RG: Regular	NO: N/A	PK: Pre K	08: Eighth Grade
RG: Regular	NO: N/A	PK: Pre K	08: Eighth Grade
RG: Regular	NO: N/A	PK: Pre K	08: Eighth Grade
RG: Regular	NO: N/A	PK: Pre K	06: Sixth Grade
RG: Regular	NO: N/A	PK: Pre K	06: Sixth Grade
RG: Regular	NO: N/A	PK: Pre K	06: Sixth Grade
RG: Regular	NO: N/A	PK: Pre K	06: Sixth Grade
RG: Regular	NO: N/A	07: Seventh Grade	08: Eighth Grade

RG: Regular	NO: N/A	07: Seventh Grade	08: Eighth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
AD: Adult	NO: N/A	AD: Adult	AD: Adult
RP: Reportable Program	NO: N/A	PK: Pre K	12: Twelfth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	06: Sixth Grade	08: Eighth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	PK: Pre K	08: Eighth Grade
AD: Adult	NO: N/A	AD: Adult	AD: Adult
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	06: Sixth Grade
RG: Regular	NO: N/A	PK: Pre K	06: Sixth Grade
RG: Regular	NO: N/A	PK: Pre K	06: Sixth Grade
RG: Regular	NO: N/A	07: Seventh Grade	08: Eighth Grade
RG: Regular	NO: N/A	06: Sixth Grade	08: Eighth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
JVC: Juvenile Correctional	NO: N/A	07: Seventh Grade	12: Twelfth Grade
AD: Adult	NO: N/A	AD: Adult	AD: Adult
CO: Correctional	NO: N/A	AD: Adult	AD: Adult
RG: Regular	NO: N/A	PK: Pre K	06: Sixth Grade
RG: Regular	NO: N/A	PK: Pre K	04: Fourth Grade
RG: Regular	NO: N/A	PK: Pre K	04: Fourth Grade
RG: Regular	NO: N/A	PK: Pre K	04: Fourth Grade
RG: Regular	NO: N/A	PK: Pre K	04: Fourth Grade
RG: Regular	NO: N/A	07: Seventh Grade	08: Eighth Grade
RG: Regular	NO: N/A	PK: Pre K	04: Fourth Grade
RG: Regular	NO: N/A	PK: Pre K	06: Sixth Grade
RG: Regular	NO: N/A	PK: Pre K	06: Sixth Grade
RG: Regular	NO: N/A	05: Fifth Grade	08: Eighth Grade
RG: Regular	NO: N/A	05: Fifth Grade	06: Sixth Grade
RG: Regular	NO: N/A	05: Fifth Grade	08: Eighth Grade
RG: Regular	NO: N/A	07: Seventh Grade	08: Eighth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade

RG: Regular	NO: N/A	PK: Pre K	12: Twelfth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
AL: Alternative	NO: N/A	07: Seventh Grade	12: Twelfth Grade
AD: Adult	NO: N/A	AD: Adult	AD: Adult
RP: Reportable Program	NO: N/A	PK: Pre K	12: Twelfth Grade
RG: Regular	NO: N/A	KG: Kindergarten	12: Twelfth Grade
RG: Regular	NO: N/A	PK: Pre K	06: Sixth Grade
RG: Regular	NO: N/A	PK: Pre K	06: Sixth Grade
RG: Regular	NO: N/A	07: Seventh Grade	08: Eighth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
AD: Adult	NO: N/A	AD: Adult	AD: Adult
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
EL: Early Learning	NO: N/A	PK: Pre K	PK: Pre K
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	06: Sixth Grade	08: Eighth Grade
RG: Regular	NO: N/A	06: Sixth Grade	08: Eighth Grade
RG: Regular	NO: N/A	06: Sixth Grade	08: Eighth Grade
RG: Regular	NO: N/A	06: Sixth Grade	08: Eighth Grade
RG: Regular	NO: N/A	06: Sixth Grade	08: Eighth Grade
RG: Regular	NO: N/A	06: Sixth Grade	08: Eighth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
AL: Alternative	NO: N/A	09: Ninth Grade	12: Twelfth Grade

AL: Alternative	NO: N/A	06: Sixth Grade	08: Eighth Grade
AL: Alternative	NO: N/A	03: Third Grade	05: Fifth Grade
AD: Adult	NO: N/A	AD: Adult	AD: Adult
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
AD: Adult	NO: N/A	AD: Adult	AD: Adult
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	DCH: District Charter	KG: Kindergarten	06: Sixth Grade
RG: Regular	NO: N/A	06: Sixth Grade	08: Eighth Grade
RG: Regular	NO: N/A	06: Sixth Grade	08: Eighth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	KG: Kindergarten	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	06: Sixth Grade	08: Eighth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
AD: Adult	NO: N/A	AD: Adult	AD: Adult
CO: Correctional	NO: N/A	AD: Adult	AD: Adult
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	06: Sixth Grade	08: Eighth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	KG: Kindergarten	08: Eighth Grade

[illegible]

[illegible]

RG: Regular	DCH: District Charter	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	06: Sixth Grade	08: Eighth Grade
RG: Regular	NO: N/A	06: Sixth Grade	08: Eighth Grade
RG: Regular	NO: N/A	06: Sixth Grade	08: Eighth Grade
RG: Regular	DCH: District Charter	KG: Kindergarten	05: Fifth Grade
RG: Regular	NO: N/A	06: Sixth Grade	08: Eighth Grade
RG: Regular	DCH: District Charter	06: Sixth Grade	08: Eighth Grade
RG: Regular	NO: N/A	06: Sixth Grade	08: Eighth Grade
RG: Regular	NO: N/A	06: Sixth Grade	08: Eighth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
AL: Alternative	NO: N/A	06: Sixth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
AL: Alternative	NO: N/A	09: Ninth Grade	12: Twelfth Grade
CTE: Career and Technical	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	PK: Pre K	12: Twelfth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	10: Tenth Grade	12: Twelfth Grade
RG: Regular	DCH: District Charter	KG: Kindergarten	08: Eighth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	DCH: District Charter	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	DCH: District Charter	09: Ninth Grade	12: Twelfth Grade
CTE: Career and Technical	NO: N/A	09: Ninth Grade	12: Twelfth Grade
EL: Early Learning	NO: N/A	PK: Pre K	PK: Pre K
EL: Early Learning	NO: N/A	PK: Pre K	PK: Pre K
SE: Special Education	NO: N/A	PK: Pre K	12: Twelfth Grade
AL: Alternative	NO: N/A	01: First Grade	12: Twelfth Grade
AD: Adult	NO: N/A	AD: Adult	AD: Adult
SE: Special Education	NO: N/A	12: Twelfth Grade	12: Twelfth Grade

AL: Alternative	NO: N/A	KG: Kindergarten	12: Twelfth Grade
RP: Reportable Program	NO: N/A	PK: Pre K	12: Twelfth Grade
RG: Regular	NO: N/A	KG: Kindergarten	05: Fifth Grade
RG: Regular	NO: N/A	03: Third Grade	06: Sixth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
RG: Regular	NO: N/A	PK: Pre K	05: Fifth Grade
EL: Early Learning	NO: N/A		
RG: Regular	NO: N/A	06: Sixth Grade	08: Eighth Grade
RG: Regular	NO: N/A	09: Ninth Grade	12: Twelfth Grade
RG: Regular	NO: N/A	06: Sixth Grade	12: Twelfth Grade
AL: Alternative	NO: N/A	09: Ninth Grade	12: Twelfth Grade
AD: Adult	NO: N/A		
RP: Reportable Program	NO: N/A		
	NO: N/A		
RG: Regular	SSC: SPCSA	KG: Kindergarten	08: Eighth Grade
RG: Regular	SSC: SPCSA	KG: Kindergarten	08: Eighth Grade
RG: Regular	SSC: SPCSA	KG: Kindergarten	08: Eighth Grade
RG: Regular	SSC: SPCSA	KG: Kindergarten	08: Eighth Grade
RG: Regular	SSC: SPCSA	PK: Pre K	05: Fifth Grade
RG: Regular	SSC: SPCSA	KG: Kindergarten	08: Eighth Grade
EL: Early Learning	NO: N/A		
EL: Early Learning	NO: N/A		
EL: Early Learning	NO: N/A		
EL: Early Learning	NO: N/A		
EL: Early Learning	NO: N/A		
EL: Early Learning	NO: N/A		
EL: Early Learning	NO: N/A		
EL: Early Learning	NO: N/A		
EL: Early Learning	NO: N/A	PK: Pre K	PK: Pre K
EL: Early Learning	NO: N/A	PK: Pre K	PK: Pre K
EL: Early Learning	NO: N/A	PK: Pre K	PK: Pre K
EL: Early Learning	NO: N/A	PK: Pre K	PK: Pre K
EL: Early Learning	NO: N/A		
RG: Regular	SSC: SPCSA	KG: Kindergarten	12: Twelfth Grade
RG: Regular	SSC: SPCSA	KG: Kindergarten	12: Twelfth Grade

RG: Regular	SSC: SPCSA	06: Sixth Grade	12: Twelfth Grade
RG: Regular	SSC: SPCSA	PK: Pre K	05: Fifth Grade
RG: Regular	SSC: SPCSA	PK: Pre K	06: Sixth Grade
RG: Regular	SSC: SPCSA	PK: Pre K	08: Eighth Grade
RG: Regular	SSC: SPCSA	PK: Pre K	08: Eighth Grade
RG: Regular	SSC: SPCSA	PK: Pre K	12: Twelfth Grade
RG: Regular	SSC: SPCSA	KG: Kindergarten	12: Twelfth Grade
RG: Regular	SSC: SPCSA	KG: Kindergarten	05: Fifth Grade
RG: Regular	SSC: SPCSA	KG: Kindergarten	12: Twelfth Grade
RG: Regular	SSC: SPCSA	04: Fourth Grade	12: Twelfth Grade
RG: Regular	SSC: SPCSA	KG: Kindergarten	08: Eighth Grade
RG: Regular	SSC: SPCSA	KG: Kindergarten	08: Eighth Grade
RG: Regular	SSC: SPCSA	KG: Kindergarten	08: Eighth Grade
RG: Regular	SSC: SPCSA	KG: Kindergarten	12: Twelfth Grade
RG: Regular	SSC: SPCSA	KG: Kindergarten	08: Eighth Grade
RG: Regular	SSC: SPCSA	KG: Kindergarten	08: Eighth Grade
RG: Regular	SSC: SPCSA	KG: Kindergarten	08: Eighth Grade
RG: Regular	SSC: SPCSA	KG: Kindergarten	05: Fifth Grade
RG: Regular	SSC: SPCSA	KG: Kindergarten	12: Twelfth Grade
RG: Regular	SSC: SPCSA	KG: Kindergarten	08: Eighth Grade
RG: Regular	SSC: SPCSA	KG: Kindergarten	08: Eighth Grade
RG: Regular	SSC: SPCSA	KG: Kindergarten	12: Twelfth Grade
RG: Regular	SSC: SPCSA	06: Sixth Grade	12: Twelfth Grade
RG: Regular	SSC: SPCSA	PK: Pre K	06: Sixth Grade
RG: Regular	SSC: SPCSA	KG: Kindergarten	05: Fifth Grade
RG: Regular	SSC: SPCSA	KG: Kindergarten	12: Twelfth Grade
RG: Regular	SSC: SPCSA	KG: Kindergarten	08: Eighth Grade
RG: Regular	SSC: SPCSA	KG: Kindergarten	12: Twelfth Grade
RG: Regular	SSC: SPCSA	PK: Pre K	08: Eighth Grade
RG: Regular	SSC: SPCSA	KG: Kindergarten	08: Eighth Grade
RG: Regular	SSC: SPCSA	KG: Kindergarten	08: Eighth Grade
RG: Regular	SSC: SPCSA	KG: Kindergarten	12: Twelfth Grade
RG: Regular	SSC: SPCSA	KG: Kindergarten	05: Fifth Grade
RG: Regular	SSC: SPCSA	KG: Kindergarten	08: Eighth Grade
RG: Regular	SSC: SPCSA	KG: Kindergarten	08: Eighth Grade

RG: Regular	SSC: SPCSA	PK: Pre K	KG: Kindergarten
RG: Regular	SSC: SPCSA	KG: Kindergarten	12: Twelfth Grade
RG: Regular	SSC: SPCSA	KG: Kindergarten	08: Eighth Grade
RG: Regular	SSC: SPCSA	06: Sixth Grade	12: Twelfth Grade
RG: Regular	SSC: SPCSA	KG: Kindergarten	08: Eighth Grade
RG: Regular	SSC: SPCSA	KG: Kindergarten	05: Fifth Grade
RG: Regular	SSC: SPCSA	06: Sixth Grade	12: Twelfth Grade
RG: Regular	SSC: SPCSA	PK: Pre K	08: Eighth Grade
RG: Regular	SSC: SPCSA	KG: Kindergarten	06: Sixth Grade
RG: Regular	SSC: SPCSA	KG: Kindergarten	08: Eighth Grade
RG: Regular	SSC: SPCSA	09: Ninth Grade	12: Twelfth Grade
RG: Regular	SSC: SPCSA	KG: Kindergarten	12: Twelfth Grade
RG: Regular	SSC: SPCSA	PK: Pre K	08: Eighth Grade
JVC: Juvenile Correctional	NO: N/A	06: Sixth Grade	12: Twelfth Grade
RG: Regular	SSC: SPCSA	11: Eleventh Grade	12: Twelfth Grade
RG: Regular	SSC: SPCSA	11: Eleventh Grade	12: Twelfth Grade
RG: Regular	SSC: SPCSA	11: Eleventh Grade	12: Twelfth Grade
RG: Regular	SSC: SPCSA	11: Eleventh Grade	12: Twelfth Grade
RG: Regular	SSC: SPCSA	11: Eleventh Grade	12: Twelfth Grade
RG: Regular	SSC: SPCSA	11: Eleventh Grade	12: Twelfth Grade
RG: Regular	SSC: SPCSA	11: Eleventh Grade	12: Twelfth Grade
RG: Regular	SSC: SPCSA	11: Eleventh Grade	12: Twelfth Grade
RG: Regular	NO: N/A	06: Sixth Grade	12: Twelfth Grade
RG: Regular	SSC: SPCSA	09: Ninth Grade	12: Twelfth Grade
RG: Regular	SSC: SPCSA	06: Sixth Grade	12: Twelfth Grade
RG: Regular	SSC: SPCSA	KG: Kindergarten	08: Eighth Grade
RG: Regular	SSC: SPCSA	PK: Pre K	08: Eighth Grade
RG: Regular	SSC: SPCSA	08: Eighth Grade	12: Twelfth Grade
RG: Regular	SSC: SPCSA	KG: Kindergarten	04: Fourth Grade
RG: Regular	SSC: SPCSA	05: Fifth Grade	07: Seventh Grade
RG: Regular	SSC: SPCSA	KG: Kindergarten	05: Fifth Grade
RG: Regular	SSC: SPCSA	KG: Kindergarten	12: Twelfth Grade
AL: Alternative	SSC: SPCSA	09: Ninth Grade	12: Twelfth Grade
RG: Regular	SSC: SPCSA	06: Sixth Grade	08: Eighth Grade
CTE: Career and Technical	SSC: SPCSA	09: Ninth Grade	12: Twelfth Grade

AL: Alternative	SSC: SPCSA	09: Ninth Grade	12: Twelfth Grade
RG: Regular	SSC: SPCSA	KG: Kindergarten	06: Sixth Grade
RG: Regular	SSC: SPCSA	KG: Kindergarten	04: Fourth Grade
RG: Regular	SSC: SPCSA	KG: Kindergarten	05: Fifth Grade
RG: Regular	SSC: SPCSA	12: Twelfth Grade	12: Twelfth Grade
RG: Regular	SSC: SPCSA	KG: Kindergarten	08: Eighth Grade
RG: Regular	SSC: SPCSA	KG: Kindergarten	08: Eighth Grade
RG: Regular	SSC: SPCSA	06: Sixth Grade	12: Twelfth Grade
RG: Regular	SSC: SPCSA	PK: Pre K	12: Twelfth Grade
RG: Regular	SSC: SPCSA	06: Sixth Grade	11: Eleventh Grade
RG: Regular	SSC: SPCSA	KG: Kindergarten	05: Fifth Grade
RG: Regular	SSC: SPCSA	KG: Kindergarten	08: Eighth Grade
RG: Regular		KG: Kindergarten	02: Second Grade

Operational Status	Principal Name	Principal Email
Open	Shannon Coombs	coombss@churchillcsd.com
Open	Brad Barton	bartonb@churchillcsd.com
Open	Kimi Melendy	melendyk@churchillcsd.com
Open	Shawn Purrell	PurrellS@Churchillcsd.com
Open	Deana Porretta	porrettad@churchillcsd.com
Open	Tim Spencer	spencert@churchillcsd.com
Open	Chantelle Redner	rednerc@churchillcsd.com
Open	Robert Hinchliffe	HINCHRW@NV.CCSD.NET
Open	Michelle Freter	freteml@nv.ccsd.net
Open	Nancy Stoops	STOOPNK@NV.CCSD.NET
Open	Shannon Lewis	lewissc@NV.CCSD.NET
Open	Traci Leigh Holloway	FENNTL@NV.CCSD.NET
Open	JEFFREY GRANGER	grangja@nv.ccsd.net
Open	Ronald Kamman	kammarw@nv.ccsd.net
Open	Jennifer L Boccia	BOCCIJL@NV.CCSD.NET
Open	Jennifer Lynn Aznarez	fenlojl@nv.ccsd.net
Open	Diana Gomez	GOMEZD1@NV.CCSD.NET
Open	Virginia H Ratliff	RATLIVH@NV.CCSD.NET
Open	LISA FERGUSON	FERGULR@NV.CCSD.NET
Open	Danielle Williams	WILLID31@NV.CCSD.NET
Open	STEPHANIE DALTON	BROWNSA@NV.CCSD.NET
Open	LAURA WILLIS	GAULTLK@NV.CCSD.NET
Open	Sarah Payne	PAYNES@NV.CCSD.NET
Open	Katie Jo Lombardo	taylokj@NV.CCSD.NET
Open	BRIANNA ROBINSON	ROBINBM@NV.CCSD.NET
Open	Audrey N Carroll	CARROAN@NV.CCSD.NET
Open	EUGENE TOYAMA	TOYAMEI@NV.CCSD.NET
Open	Michelle Nicole Schuebel	SCHUEMN@NV.CCSD.NET
Open	Annemarie Stover	CLARKAD@NV.CCSD.NET
Open	Kody M Barto	BARTOKM@NV.CCSD.NET
Open	Sarah Cyprus	VANDOSJ@NV.CCSD.NET
Open	Ashley Martin	MARTIA31@NV.CCSD.NET
Open	Victoria Turner	turnevd1@nv.ccsd.net
Open	Isabelle Sanchez Ager	SANCHIM@NV.CCSD.NET

Open	Nakia Barker	BARKEN@NV.CCSD.NET
Open	Heather G Skramstad	FORDHG@NV.CCSD.NET
Open	Renee Mechem	MECHERJ@NV.CCSD.NET
Open	Jeanette Taylor	BENDEJC@NV.CCSD.NET
Open	SANDRA BAEZA	VALDISG@NV.CCSD.NET
Open	Amy E Yee	YEEAE@NV.CCSD.NET
Open	CHRISTINE VASQUEZ	VASQUCM@NV.CCSD.NET
Open	Jennifer Gerber	MENGJA@NV.CCSD.NET
Open	Shannon Williamson	WILLISL4@NV.CCSD.NET
Open	Heather Rose Fonte	FONTEHR@NV.CCSD.NET
Open	Christine Vasquez	VASQUCM@NV.CCSD.NET
Open	Christopher Welch	WELCHCJ@NV.CCSD.NET
Open	Tracy Echeverria	ECHEVTD@NV.CCSD.NET
Open	Douglas Taylor	TAYLODH@NV.CCSD.NET
Open	Jessica Robbins	robbija@nv.ccsd.net
Open	Kelly Prellwitz	FAWCEK@NV.CCSD.NET
Open	Jennifer Krizmanic	WARDJD@NV.CCSD.NET
Open	Karen Collins	COLLIKD@NV.CCSD.NET
Open	Cynthia M Marlowe	MARLOCM@NV.CCSD.NET
Open	Andrea Hill	HILLAM@NV.CCSD.NET
Open	Rebecka D Christensen	CHRISRD@NV.CCSD.NET
Open	Nikki Longmore	LONGMNJ@NV.CCSD.NET
Open	Kelby Robison	ROBISKR@NV.CCSD.NET
Open	Alan Alden	ALDENAJ@NV.CCSD.NET
Open	Anna Cool-Macrae	COOLMA@NV.CCSD.NET
Open	Brandi Kulin	KULINBA@NV.CCSD.NET
Open	Stephanie Ann MacDuffee	BOURGSA@NV.CCSD.NET
Open	SHANNON PASH	GLEASSN@NV.CCSD.NET
Open	Blair Rodrigues	DOTTABC@NV.CCSD.NET
Open	Margaret E Newman	NEWMAME@NV.CCSD.NET
Open	Jennifer L Reynolds	REYNOJL@NV.CCSD.NET
Open	Donald McKinney	MCKINDA1@NV.CCSD.NET
Open	Debra Huckins	HUCKIDL@NV.CCSD.NET
Open	BRIONE MINOR-MITCHELL	MINORBA@NV.CCSD.NET
Open	Andrea Heinlen	HEINLAM@NV.CCSD.NET

Open	Erin Nguyen	waverem@NV.CCSD.NET
Open	Carla Buchanan	BUCHACA@NV.CCSD.NET
Open	Denise Hill	gabredr@nv.ccsd.net
Open	Cheryle L Trupp	truppcl@nv.ccsd.net
Open	Jennifer Lynn Renville	RENVIJ@NV.CCSD.NET
Open	Bridget K Leatherman	LEATHBK@NV.CCSD.NET
Open	Rachelle Duggins-Tetlow	DUGGIRA@NV.CCSD.NET
Open	Rachel Dipaolo	DIPAORR@NV.CCSD.NET
Open	Christina M Miani	MIANICM@NV.CCSD.NET
Open	Jason Schrock	SCHROJW@NV.CCSD.NET
Open	Brodie C Christian	CHRISBC@NV.CCSD.NET
Open	Kari Creamer	GILLAKM@NV.CCSD.NET
Open	AMANDA RAE DAVIS	DAVISAR@NV.CCSD.NET
Open	Kathi-Anne Rozek	ROZEKK@NV.CCSD.NET
Open	Gina Campbell	MARTIGL@NV.CCSD.NET
Open	Dena Pritchett	HOLNBDM@NV.CCSD.NET
Open	Frederick E Watson	WATSOFE@NV.CCSD.NET
Open	STEPHANIE TATMAN	TATMASA@NV.CCSD.NET
Open	David C Hudzick	HUDZIDC@NV.CCSD.NET
Open	MEAGHAN MCGOWAN	MCGOWME@NV.CCSD.NET
Open	Melissa Ramirez	RAMIRML@NV.CCSD.NET
Open	Brandi Mora	MORABE@NV.CCSD.NET
Open	Debra L Jones	JONESDL3@NV.CCSD.NET
Open	MARISSA RASAVONG	RASAVML@NV.CCSD.NET
Open	Juanita B Frasier	FRASIJB@NV.CCSD.NET
Open	Jennifer A French	FRENCJA@NV.CCSD.NET
Open	Jane Fernandez	fernajb@NV.CCSD.NET
Open	Ronda Reedom	REEDORC@NV.CCSD.NET
Open	Brandi Pineda	PINEDBL@NV.CCSD.NET
Open	Laurence J Derasmo	deraslj@nv.ccsd.net
Open	David Kirkhart	KIRKHDL@NV.CCSD.NET
Open	Michael Dobbyn	DOBBYMD@NV.CCSD.NET
Open	Christopher A Jenkins	JENKICA@NV.CCSD.NET
Open	ROBERT ROSENBLATT	ROSENRB@NV.CCSD.NET
Open	LISA MEO	WILLILM3@NV.CCSD.NET

Open	JAIME WITTE	WITTEJL@NV.CCSD.NET
Open	Merrill Young	YOUNGML@NV.CCSD.NET
Open	Christina M Stacey	STACECM@NV.CCSD.NET
Open	LIN SORIANO	CLEGGLB@nv.ccsd.net
Open	Jonathan Yutuc	yutucje@nv.ccsd.net
Open	Lalara Laster	SWANSLS@NV.CCSD.NET
Open	Lindsay Packer	PACKELK@NV.CCSD.NET
Open	Kelly L Wright	WRIGHKL@NV.CCSD.NET
Open	Traci McLaughlin	MCLAUTL@NV.CCSD.NET
Open	Tenisha Renee Brunetti	SIMMOTR@NV.CCSD.NET
Open	Kimberly Gray	MORRIKA@NV.CCSD.NET
Open	Mike N Houle	HOULEMN@NV.CCSD.NET
Open	Jennifer L Hamby	hambyjl@nv.ccsd.net
Open	Jennifer Haynal	HAYNAJ@NV.CCSD.NET
Open	Misty Tyler	tylerma@nv.ccsd.net
Open	Shawn C Nielsen	NIELSSC@NV.CCSD.NET
Open	Todd A Lindberg	LINDBTA@NV.CCSD.NET
Open	Kenneth Weaver	weavek@nv.ccsd.net
Open	JODI NOTCH	NOTCHJL@NV.CCSD.NET
Open	Sarah Robinson	ROBINSM3@NV.CCSD.NET
Open	KENT SABO	SABOKE@NV.CCSD.NET
Open	Toni-Ann Perales	LOMBAT@NV.CCSD.NET
Open	KAREN MARENTIC	MARENKT@NV.CCSD.NET
Open	Daniel R Hungerford	HUNGEDR@NV.CCSD.NET
Open	Heather Hawley	HAWLEHM@NV.CCSD.NET
Open	Nicole Bryan	BRYANNM@NV.CCSD.NET
Open	Kristy M Muffoletto	CONLEKM@NV.CCSD.NET
Open	Karen S Thomasson	KROLKS@NV.CCSD.NET
Open	Pamela Catano	catanpa@nv.ccsd.net
Open	Angela Jefferson	JEFFFEAK@NV.CCSD.NET
Open	Shalynn Tinkel	tinkesn@NV.CCSD.NET
Open	Christopher J Sparrow	SPARRCJ@NV.CCSD.NET
Open	Adrian M Quinonez	QUINOAM@NV.CCSD.NET
Open	Kim Barra	BARRAKR@NV.CCSD.NET
Open	Heather J Lenz	LENZHJ@NV.CCSD.NET

Open	Jill Fisher	prineja@nv.ccsd.net
Open	Jill Snyder	SNYDEJM1@NV.CCSD.NET
Open	TAMRA BROOKS	BROOKTL@NV.CCSD.NET
Open	Kimberly Fundaro	FUNDAKA@NV.CCSD.NET
Open	Holly Lawrence	SHAFFHE@NV.CCSD.NET
Open	Melissa Giannantonio	GIANNMS@NV.CCSD.NET
Open	Michelee Q Crawford	CRAWFMQ@NV.CCSD.NET
Open	TIFFANY R BURLACU	millete@nv.ccsd.net
Open	Karin L Kip	KIPKL@NV.CCSD.NET
Open	Deborah Annette Faltinosky	FALTID@NV.CCSD.NET
Open	Frances Lucero	LUCERFV@NV.CCSD.NET
Open	Lori J Andrews	ANDRELJ1@NV.CCSD.NET
Open	Michelle Wheatfill	WHEATMA@NV.CCSD.NET
Open	Cecilia Bojorquez	bojorc@NV.CCSD.NET
Open	Cullen Skyles	SKYLECT@nv.ccsd.net
Open	Frances Mariselle Castillo	CABUHFM@NV.CCSD.NET
Open	Brandon J Danowski	DANOWBJ@NV.CCSD.NET
Open	ALEX TEJERO	TEJERA@NV.CCSD.NET
Open	Elizabeth Poglitsch	LEMIEEE@NV.CCSD.NET
Open	JENNIFER BENIZIO	BENIZJL@NV.CCSD.NET
Open	Michelle Matthews	MATTHM@NV.CCSD.NET
Open	Allison Pokornik	BRUEGAM@NV.CCSD.NET
Open	Ayoka M Snipes	SNIPEAM@NV.CCSD.NET
Open	Deborah Young Yock	YOUNGDK@NV.CCSD.NET
Open	Jeffrey Schaber	schabj@nv.ccsd.net
Open	Jensie Ogiela-Stroh	OGIELJT@NV.CCSD.NET
Open	Jackie Wyett	WYETTJL@NV.CCSD.NET
Open	Krystal Childress	WILLEKL@NV.CCSD.NET
Open	Rajul Edmond	EDMONRD@NV.CCSD.NET
Open	Jerrell D Hall	WILLIJD1@NV.CCSD.NET
Open	Delilah Krasch	KRASCDJ@NV.CCSD.NET
Open	Cecilia Harge	HARGE@NV.CCSD.NET
Open	Tara Garman Doetch	SPEAKTL@NV.CCSD.NET
Open	Wendy B De Mille	DEMILWB@NV.CCSD.NET
Open	Pamela Johnson	JOHNSPC@NV.CCSD.NET

Open	Ellen M Stayman	STAYMEM@NV.CCSD.NET
Open	Amanda Lush	LUSHAK@NV.CCSD.NET
Open	Chantae Rreadye	READYC@NV.CCSD.NET
Open	Jaymes A Aimetti	AIMETJA@NV.CCSD.NET
Open	PAOLA ELENA ZEPHER	MAUROPE@NV.CCSD.NET
Open	Hilary Eisen	EISENHA@NV.CCSD.NET
Open	Michael Stosek	STOSEM@NV.CCSD.NET
Open	Nicole Baumgartner	MIDYENI@NV.CCSD.NET
Open	Carrie A Reasbeck	REASBCA@NV.CCSD.NET
Open	Katie Rankin	RANKIKA@NV.CCSD.NET
Open	LA TONYA JUNIEL-SWANSON	JUNIELR@NV.CCSD.NET
Open	Laura Turner	TURNELR@NV.CCSD.NET
Open	Stanica Sretenovic	sretes@nv.ccsd.net
Open	Casandra Woodall	WOODACN@NV.CCSD.NET
Open	Shannon C Brown	BROWNSC@NV.CCSD.NET
Open	Jennifer Furman Born	FURMAJM@NV.CCSD.NET
Open	Tracy Echeverria	ECHEVTD@NV.CCSD.NET
Open	Heather Synold	HENDEHM@NV.CCSD.NET
Open	Christopher Welch	WELCHCJ@NV.CCSD.NET
Open	Tamara Bonica	BONICT@NV.CCSD.NET
Open	Kimberly S Basham	BASHAKS@NV.CCSD.NET
Open	Matthew P Bennett	BENNEMP@NV.CCSD.NET
Open	Andrea Tarrant	GRAYAL@NV.CCSD.NET
Open	Margaret K Putnam	PUTNAMK@NV.CCSD.NET
Open	Gregory Winiewicz	WINIEGS@NV.CCSD.NET
Open	Kimberly M Swoboda	SWOBOKM@NV.CCSD.NET
Open	Morgan McGaha	MCGAHMW@NV.CCSD.NET
Open	Magdalena Casillas	CASILM@NV.CCSD.NET
Open	ANTHONY WHITE	WHITEAJ@NV.CCSD.NET
Open	Taryn Apollo	TROMBTA@NV.CCSD.NET
Open	Jennifer Wright	myersjl@nv.ccsd.net
Open	Heather Wiedenheft	WIEDEHD@NV.CCSD.NET
Open	Terri Castillo	CASTITL1@NV.CCSD.NET
Open	Shannon Lively	LIVELS@NV.CCSD.NET
Open	Tammy R Villarreal Crabb	VILLATR@NV.CCSD.NET

Open	Jordana McCudden	MCCUDJJ@NV.CCSD.NET
Open	Rigel A Painter	paintra@nv.ccsd.net
Open	Vanessa M Altfas	ALTFAVM@NV.CCSD.NET
Open	Jeannine Anderson	ANDERJN@NV.CCSD.NET
Open	Staca B Sadie	SADIESB@NV.CCSD.NET
Open	Lene N Muth	MUTHLN@NV.CCSD.NET
Open	Tracey Christine Collins	ROEHNTC@NV.CCSD.NET
Open	Barbara Griffin	GRIFFB3@NV.CCSD.NET
Open	Nicole Leighton	leighn@NV.CCSD.NET
Open	Ashley Gannon	MITCHAR@NV.CCSD.NET
Open	KELBY ROBISON	ROBISKR@NV.CCSD.NET
Open	Kevin P Gilmore	GILMOKP@NV.CCSD.NET
Open	Timothy D Adams	ADAMSTD@NV.CCSD.NET
Open	Shiah Littmann	LITTMSD@NV.CCSD.NET
Open	Melissa L Baker	BAKERML1@NV.CCSD.NET
Open	Angela R Shepard	SHEPAAR@NV.CCSD.NET
Open	Monica Brown	TAYLOML2@NV.CCSD.NET
Open	JAYMI CLEMENS	CLEMEJT@NV.CCSD.NET
Open	Linnea Westwood	WESTWL@NV.CCSD.NET
Open	ROSALYNDA ODOM	SWEENRS@NV.CCSD.NET
Open	Amy A Godinez	GODINAA@NV.CCSD.NET
Open	Tammy Flanagan	REYNOTJ@NV.CCSD.NET
Open	Jonathan Moss	MOSSJM@NV.CCSD.NET
Open	LAKEISHA MYERS	MYERSLO@NV.CCSD.NET
Open	Sarah Udy	UDYSM@NV.CCSD.NET
Open	Timothy Jessesky	JESSETJ@NV.CCSD.NET
Open	VERONICA HUNT	HUNTVA@NV.CCSD.NET
Open	David Copenbarger	COPENDM@NV.CCSD.NET
Open	Darla D Richards	RICHADD@NV.CCSD.NET
Open	MEAGAN LEWIS	LEWISMM@NV.CCSD.NET
Open	Cecilia Harge	HARGE@NV.CCSD.NET
Open	Matthew Spurk	SPURKMA@NV.CCSD.NET
Open	Georgena Kubiak Reagh	REAGHG@NV.CCSD.NET
Open	Rachel Samuel	MANOHRJ@NV.CCSD.NET
Open	Hallie Loewy	FIKEHE@NV.CCSD.NET

Open	Maria Switzer	YODERMA@nv.ccsd.net
Open	Ramona Fricker	FRICKRG@NV.CCSD.NET
Open	Abigail Johnson	ALLISAS@NV.CCSD.NET
Open	Harold Bashay	BASHAHK@NV.CCSD.NET
Open	Christopher Gist	GISTC@NV.CCSD.NET
Open	Deborah Thaggard	THAGGD@NV.CCSD.NET
Open	Sara Friedman	FRIEDSH@NV.CCSD.NET
Open	Christopher L Hermes	HERMECL@NV.CCSD.NET
Open	Buffy Banks-Grove	banksbt@NV.CCSD.NET
Open	Leslye Galvin	GALVILD@NV.CCSD.NET
Open	Erin Rolfe	ROLFEE@NV.CCSD.NET
Open	Melanie Teemant	teemamj@nv.ccsd.net
Open	Jason Kathan	KATHAJM@NV.CCSD.NET
Open	Tammy Flanagan	REYNOTJ@NV.CCSD.NET
Open	Dawn L Estes	ESTESDL@NV.CCSD.NET
Open	Kennie Churchwell	CHURCK@NV.CCSD.NET
Open	Trudi Jacobs	JACOBTK@NV.CCSD.NET
Open	Jacqueline L Carducci	CARDUJL@NV.CCSD.NET
Open	Teresa Evans	SINGLT@NV.CCSD.NET
Open	Matthew Jackson	JACKSMW@NV.CCSD.NET
Open	Philicia King-Spenard	KINGPL1@NV.CCSD.NET
Open	Brandy Kirkpatrick	KIRKPBD@NV.CCSD.NET
Open	Almee Lewis	LEWISAD@NV.CCSD.NET
Open	Nakia Barker	BARKEN@NV.CCSD.NET
Open	Kelly Thorson	THORSKT@NV.CCSD.NET
Open	Brittney Elaine Nuanez	CANNABE@NV.CCSD.NET
Open	Spencer A Beals	BEALSSA@NV.CCSD.NET
Open	Yvette M. Tippetts	JAGGEYM@nv.ccsd.net
Open	Edward San Nicolas	SANNIEP@NV.CCSD.NET
Open	Christopher Welch	WELCHCJ@NV.CCSD.NET
Open	Allen Yee	YEEAG@NV.CCSD.NET
Open	Joshua Wikler	WIKLEJA@NV.CCSD.NET
Open	Susan J Harrison	HARRISJ@NV.CCSD.NET
Open	Lana Roper	ROPERLM@NV.CCSD.NET
Open	Gary B Bugash	BUGASGB@NV.CCSD.NET

Open	Uriel Garcia Escudero	GARCIUM@NV.CCSD.NET
Open	Terri Knepp	KNEPPTK@NV.CCSD.NET
Open	La Toya Jordan Brown	jordall@nv.ccsd.net
Open	Phongsavanh Skvarek	SKVARP@nv.ccsd.net
Open	Greg Siqueiros	SIQUEGP@NV.CCSD.NET
Open	Christie Ford	FORDCA@NV.CCSD.NET
Open	Jaclyn Ayala	BRANDJ@NV.CCSD.NET
Open	Jaydel Wilson	WILSOJE@NV.CCSD.NET
Open	FRANCISCO GARCIA	GARCIF@NV.CCSD.NET
Open	Eliza Perez	PEREZE21@NV.CCSD.NET
Open	Bradley Leimbach	leimbbw@NV.CCSD.NET
Open	Heather Mounts	MOUNTHL@NV.CCSD.NET
Open	Brentley Garbutt	BRIDGBA1@NV.CCSD.NET
Open	Danielle Duterte	DUTERDD@NV.CCSD.NET
Open	Melonie Poster	POSTEMR@NV.CCSD.NET
Open	TONYA ROSE	ROSETL@NV.CCSD.NET
Open	Brian Brill	BRILLB@NV.CCSD.NET
Open	Roger D West	WESTRD@NV.CCSD.NET
Open	Pamela Lindemuth	nortopm@nv.ccsd.net
Open	Michelle Matthews	MATTHM@NV.CCSD.NET
Open	Zeola Braxton	BRAXTZE@NV.CCSD.NET
Open	Raymond Ortiz	ORTIZR1@nv.ccsd.net
Open	Norman Smith	SMITHNE1@NV.CCSD.NET
Open	Kimberly Perry-Carter	PERRYKK1@NV.CCSD.NET
Open	Antonio Rael	RAELA@NV.CCSD.NET
Open	Mohammad Hadavi	HADAVMT@NV.CCSD.NET
Open	Stacey L White	WHITESL@NV.CCSD.NET
Open	Kristal Cummings	CUMMIKN@NV.CCSD.NET
Open	Christina Brockett	BROCKCK@NV.CCSD.NET
Open	Brian Wiseman	WISEMBR@NV.CCSD.NET
Open	Isabelle Sanchez Ager	SANCHIM@NV.CCSD.NET
Open	Colin Mcnaught	MCNAUCE@NV.CCSD.NET
Open	Anthony Nunez	NUNEZAM1@NV.CCSD.NET
Open	Kent A Roberts	ROBERKA1@NV.CCSD.NET
Open	Stacie Nelson	NELSOSA2@NV.CCSD.NET

Open	Lezlie Korpp	KOEPPLS@NV.CCSD.NET
Open	Walter Shappley	SHAPPW@NV.CCSD.NET
Open	Jaime M Ditto	DITTOJM@NV.CCSD.NET
Open	Stephanie Machin	MACHIS@nv.ccsd.net
Open	Stephanie Machin	MACHIS@nv.ccsd.net
Open	Gregory L Cole	COLEGL@NV.CCSD.NET
Open	Lisa Schumacher	CAMPBLM1@NV.CCSD.NET
Open	Stephanie Machin	MACHIS@nv.ccsd.net
Open	Traci Kannon	KANNOTK@NV.CCSD.NET
Open	Megan Sensinaugh	SENSIMA@NV.CCSD.NET
Open	Adam Canfield	CANFIAM@NV.CCSD.NET
Open	Nadia Steger	STEGENJ@NV.CCSD.NET
Open	TARA POWELL	POWELTB@NV.CCSD.NET
Open	Joshua Davis	DAVISJB@NV.CCSD.NET
Open	Donna M Levy	LEVYDM@NV.CCSD.NET
Open	Dawn Martin	MARTID20@NV.CCSD.NET
Open	Amy C Dockter Rozar	DOCKTAC@NV.CCSD.NET
Open	Megan Sensibaugh	SENSIMA@NV.CCSD.NET
Open	Amy C Wagner	WAGNEAC@NV.CCSD.NET
Open	Duane McMin	MCMINDE@NV.CCSD.NET
Open	Stephen Waite	WAITESD@NV.CCSD.NET
Open	Christopher Welch	WELCHCJ@NV.CCSD.NET
Open	Keith Wiperman	WIPPEKM@NV.CCSD.NET
Open	Jonathan Synold	SYNOLJJ@NV.CCSD.NET
Open	Shirley Jimenez	JIMENSJ@NV.CCSD.NET
Open	Jessica Lee Lovell	LOVELJL3@NV.CCSD.NET
Open	Michael N Piccininni	PICCIMN@NV.CCSD.NET
Open	Duane Bickmore	BICKMDK1@NV.CCSD.NET
Open	BELINDA MARENTIC	MARENBM@NV.CCSD.NET
Open	LAURA WILLIS	GAULTLK@NV.CCSD.NET
Open	Ian Salzman	SALZMIM@nv.ccsd.net
Open	Natasha Lerutte	LERUTNG@NV.CCSD.NET
Open	Michael Martin	MARTIMH@NV.CCSD.NET
Open	Michael Martin	MARTIMH@NV.CCSD.NET
Open	Lilianna Bonderov	bondelm@nv.ccsd.net

Open	Ryan Cordia	cordird@nv.ccsd.net
Open	Anne Harper	harpeae@nv.ccsd.net
Open	Gina Piccolo	piccog@nv.ccsd.net
Open		
Open	Pate Thomas	thomapr1@nv.ccsd.net
Open	Anthony Nunez	NUNEZAM1@NV.CCSD.NET
Open	Colin Mcnaught	MCNAUCE@NV.CCSD.NET
Open	Shirley Jimenez	JIMENSJ@NV.CCSD.NET
Open	Antonio Rael	RAELA@NV.CCSD.NET
Open	Brian Wiseman	WISEMBR@NV.CCSD.NET
Open	Palmer Jackson	JACKSPD1@NV.CCSD.NET
Open	Jason L Fico	FICOJL1@NV.CCSD.NET
Open	Gina Piccolo	PICCOG@NV.CCSD.NET
Open	Johsua B Katz	KATZJB@NV.CCSD.NET
Open	Rebecca Vandepol	MURRAR@NV.CCSD.NET
Open	Rebecca Vandepol	MURRAR@NV.CCSD.NET
Open	LEILANI IRENE SHIVE	SHIVEL@NV.CCSD.NET
Open	Amy Miller	MILLEAE2@NV.CCSD.NET
Open	Royal Goebel	GOEBERJ@NV.CCSD.NET
Open	Kamille Bryner	BRYNEKA@NV.CCSD.NET
Open	Joanne Vattiato	VATTIJM@nv.ccsd.net
Open	Joanne Vattiato	VATTIJM@nv.ccsd.net
Open	David Monroe	MONRODC@NV.CCSD.NET
Open	Robert Lee	LEER13@NV.CCSD.NET
Open	Michael Sharapan	SHARAMS@NV.CCSD.NET
Open	Jason L Fico	FICOJL1@NV.CCSD.NET
Open	Gina Piccolo	piccog@nv.ccsd.net
Open	Gina Piccolo	piccog@nv.ccsd.net
Open	Michael Rolands	ROLANMA@NV.CCSD.NET
Open	Ryan Lewis	LEWISRJ@nv.ccsd.net
Open	Margaret Froby	FROBYM@NV.CCSD.NET
Open	LEILANI IRENE SHIVE	SHIVEL@NV.CCSD.NET
Open	Janice Polley Augente	POLLEJ@NV.CCSD.NET
Open	Michael Rolands	ROLANMA@NV.CCSD.NET
Open	Angela Nickels	NICKEAM@NV.CCSD.NET

Open	Amy Manning	MANNIAM@NV.CCSD.NET
Open	Edward Sikora	sikore@nv.ccsd.net
Open	Gina Piccolo	piccog@nv.ccsd.net
Open	Veronica Griffith	vgriiffth@dcsd.k12.nv.us
Open	Sean Ryan	sryan@dcsd.k12.nv.us
Open	Heather Duncan	hduncan@dcsd.k12.nv.us
Open	Blaine Spires	bspires@dcsd.k12.nv.us
Open	Jason Reid	jreid@dcsd.k12.nv.us
Open	Andrew Fromdahl	afromdah@dcsd.k12.nv.us
Open	Greg Thetford	gthetford@dcsd.k12.nv.us
Open	Amy Carter	acarter@dcsd.k12.nv.us
Open	Michael Rechs	mrechs@dcsd.k12.nv.us
Open	Alicia Braaksma	abraaksm@dcsd.k12.nv.us
Open	Stormy Herald	sherald@dcsd.k12.nv.us
Open	Stormy Herald	sherald@dcsd.k12.nv.us
Open	Stormy Herald	sherald@dcsd.k12.nv.us
Open	Mike Rechs	mrechs@dcsd.k12.nv.us
Open	Stormy Herald	sherald@dcsd.k12.nv.us
Open	Amy Kidman-Delaney	akidman@dcsd.k12.nv.us
Open	Jeffrey Revier	jrevier@ecsdnv.net
Open	Stormi McCarthy	smccarthy@ecsdnv.net
Open	Patrick DiSpirito	pdispirito@ecsdnv.net
Open	Jessica Harris	jharris2@ecsdnv.net
Open	Angela Silva	asilva3@ecsdnv.net
Open	Bobby Steensen	bsteense@ecsdnv.net
Open	Sean Stanton	sstanton@ecsdnv.net
Open	Jeffrey Revier	jrevier@ecsdnv.net
Open	Thomas Cunningham	tcunning@ecsdnv.net
Open	Mauro Lobato	mlobato@ecsdnv.net
Open	Lynn Manning John	lmanningjohn@ecsdnv.net
Open	Angela Silva	asilva3@ecsdnv.net
Open	Patrick DiSpirito	pdispirito@ecsdnv.net
Open	Cynthia Etchemendy	cetchemendy@ecsdnv.net
Open	Chrissie Blanchard	cblanchard@ecsdnv.net
Open	Jessica Harris	jharris2@ecsdnv.net

Open	Travis Monett	tmonett@ecsdnv.net
Open	Mauro Lobato	mlobato@ecsdnv.net
Open	Angela Silva	asilva3@ecsdnv.net
Open	Jennifer Gohl	jgohl@ecsdnv.net
Open	Salli McDermott	smcdermo@ecsdnv.net
Open	Stormi McCarthy	smccarthy@ecsdnv.net
Open	Lynn Manning John	lmanningjohn@ecsdnv.net
Open	Gregory Smith	gsmith@ecsdnv.net
Open	Mauro Lobato	mlobato@ecsdnv.net
Open	Angela Silva	asilva3@ecsdnv.net
Open	Jonathan Foss	jfoss@ecsdnv.net
Open	Lynn Manning John	lmanningjohn@ecsdnv.net
Open	Stormi McCarthy	smccarthy@ecsdnv.net
Open	Wade Pehrson	wpehrson@ecsdnv.net
Open	Jared Holloway	jholloway@ecsdnv.net
Open	Emily Nielson	enielson@ecsdnv.net
Open	Emily Nielson	enielson@ecsdnv.net
Open	Aaron Fisher	afisher@ecsdnv.net
Open	Aaron Fisher	afisher@ecsdnv.net
Open	Justin Streeter	jstreeter@ecsdnv.net
Open	Jonathan Firme	jfirme@ecsdnv.org
Open	Jonathan Firme	jfirme@ecsdnv.org
Open	Jonathan Firme	jfirme@ecsdnv.org
Open	Steven Sullivan	ssullivan@eureka.k12.nv.us
Open	Steven Sullivan	ssullivan@eureka.k12.nv.us
Open	John Glover	yglover@eureka.k12.nv.us
Open	Leslie Molina	lmolini@hcsdnv.com
Open	Leslie Molina	lmolina@hcsdnv.com
Open	Leslie Molina	lmolina@hcsdnv.com
Open	Leslie Molina	lmolina@hcsdnv.com
Open	Chelsea Cabatbat	ccabatbat@hcsdnv.com
Open	Rebecca Fitzgerald	rfitzgerald@hcsdnv.com
Open	Rob Lindsay	rlindsay@hcsdnv.com
Open	Clay Sagers	csagers@hcsdnv.com
Open	Jen Evans	jevans@hcsdnv.com

Open	Rob Lindsay	rlindsay@hcsdnv.com
Open	Shaun Taylor	staylor@hcsdnv.com
Open	Rob Lindsay	rlindsay@hcsdnv.com
Open	Leslie Molina	lmolina@hcsdnv.com
Open		
Open	Kim Willis	Kwillis@landernv.net
Open	Jacqueline Buchel	jbuchel@landernv.net
Open	Cori Warwood	cwarwood@landernv.net
Open	Amber Gandolfo	Agandolfo@landernv.net
Open	Carly Robertson	crobertson@landernv.net
Open	Mike Sparrow	msparrow@lcsdnv.com
Open	Doug Peterson	dpeterson@lcsdnv.com
Open	Raymond Wadsworth	rwadsworth@lcsdnv.com
Open	Stephanie Vincent	svincent@lcsdnv.com
Open	Dr. Michael Roth	mroth@lcsdnv.com
Open	Brooke Foremaster	bforemaster@lcsdnv.com
Open	Sharon Dirks	sdirks@lcsdnv.com
Open	Brooke Foremaster	bforemaster@lcsdnv.com
Open	MaCall Barnes	mbarnes@lcsdnv.com
Open	Cherry Florence	cflorence@lcsdnv.com
Open	Cherry Florence	cflorence@lcsdnv.com
Open	Chase Woodford	cwoodford@lyoncsd.org
Open	Rich Fortier	Rich.Fortier@lyoncsd.org
Open	Jaime Henderson	jsmith@lyoncsd.org
Open	Erin Korf	ekorf@lyoncsd.org
Open	Kent Jones	kentjones@lyoncsd.org
Open	Kevin Kranjcec	kkranjcec@lyoncsd.org
Open	Virginia Richardson	vrichardson@lyoncsd.org
Open	Corinne Burns	cburns@lyoncsd.org
Open	Rachel Kuhn	rkuhn@lyoncsd.org
Open	Scott Gillespie	sgillespie@lyoncsd.org
Open	Reema Pulsifer	rpulsifer@lyoncsd.org
Open	Jed Marciniak	jmarciniak@lyoncsd.org
Open	Steve Henderson	shenderson@lyoncsd.org
Open	Ryan Cross	rcross@lyoncsd.org

Open	Stephanie Coplan	scoplan@lyoncsd.org
Open	Kathy Bomba-Edgerton	kbomba-edgerton@lyoncsd.org
Open	Julie Bumgardner	jbumgardner@lyoncsd.org
Open	Amber Cross	amber.cross@lyoncsd.org
Open	Amber Cross	amber.cross@lyoncsd.org
Open	Jim Gianotti	jimgianotti@lyoncsd.org
Open	Rachel Stewart	rstewart@lyoncsd.org
Open	Chanen Cross	ccross@lyoncsd.org
Open	Claire Hayhurst	hayhurst.claire@nvmcsd.org
Open	Lance West	west.lance@nvmcsd.org
Open	Monica Keady	keady.monica@nvmcsd.org
Open	Monica Keady	keady.monica@nvmcsd.org
Open	Maryjo Gemelke	gemelke.maryjo@nvmcsd.org
Open	Samantha Moore	sdmoore@nyeschools.org
Open	Thaddeus Wind	twind@nyeschools.org
Open	Holly Riggs	hriggs@nyeschools.org
Open	Amanda Arceo	aarceo@nyeschools.org
Open	Sylvia DeMasi	sdemasi@nyeschools.org
Open	Andrew Jones	ajones@nyeschools.org
Open	Timothy Wombaker	twombaker@nyeschools.org
Open	Elizabeth Gilligan	egilligan@nyeschools.org
Open	Jared Peruch	jperuch@nyeschools.org
Open	Greg Bailey	gbailey@nyeschools.org
Open	April Sutton	asutton@nyeschools.org
Open	Andrew Jones	ajones@nyeschools.org
Open	Timothy Wombaker	twombaker@nyeschools.org
Open	Thaddeus Wind	twind@nyeschools.org
Open	Holly Riggs	hriggs@nyeschools.org
Open	Amanda Arceo	aarceo@nyeschools.org
Open	Andrew Jones	ajones@nyeschools.org
Open	Holly Riggs	hriggs@nyeschools.org
Open	Timothy Wombaker	twombaker@nyeschools.org
Open	Desiree Veloz	dveloz@nyeschools.org
Open	Thaddeus Wind	twind@nyeschools.org
Open	Holly Riggs	hriggs@nyeschools.org

Open	Holly Riggs	hriggs@nyeschools.org
Open	Holly Riggs	hriggs@nyeschools.org
Open	Holly Riggs	hriggs@nyeschools.org
Open	Cheryl Richetta	Crichetta@carson.k12.nv.us
Open	Robert Chambers	Rchambers@carson.k12.nv.us
Open	Daniel Brown	dbrown@carson.k12.nv.us
Open	Jennifer Conmay	Jconmay@carson.k12.nv.us
Open	Kari Pryor	Kpryor@carson.k12.nv.us
Open	Raegan Virgil	Rvirgil@carson.k12.nv.us
Open	Chelise Crookshanks	Ccrookshanks@carson.k12.nv.us
Open	Sarah Lobsinger	Slobsinger@carsonmontessori.com
Open	Mark Robinson	Mrobinson@carson.k12.nv.us
Open	Gina Hoppe	Ghoppe@carson.k12.nv.us
Open	Daniel Carstens	Dcarstens@carson.k12.nv.us
Open	William Harvey	wharvey@pcsdnv.com
Open	William Harvey	wharvey@pcsdnv.com
Open	Jonathan Reynolds	jreynolds@pcsdnv.com
Open	Shea Murphy	smurphy@pcsdnv.com
Open		
Open		
Open	Sonja Hess	shess@storeynv.com
Open	Sonja Hess	shess@storeynv.com
Open	Cody Farnworth	cfarnworth@storeynv.com
Open	Cody Farnworth	cfarnworth@storeynv.com
Open	Kevin Sady	ksady@washoeschools.net
Open	Marcus Culpepper	MaCulpepper@WashoeSchools.net
Open	Jessica Wilson	JNWilson@washoeschools.net
Open	RYAN SMITH	RGSmith@washoeschools.net
Open	Barbara Surritte-Barker	BHBarker@washoeschools.net
Open	Amanda McWilliams	AMcWilliams@washoeschools.net
Open	Ryan Smith	Ryan.Smith@WashoeSchools.net
Open	Mary Culpepper	mculpepper@WashoeSchools.net
Open	Kristina Martin	KMartin@washoeschools.net
Open	Jeff Batavia	JBatavia@washoeschools.net
Open	Richard Mares	RMares@washoeschools.net

Open	HEATHER THAXTON	HThaxton@washoeschools.net
Open	Amy Howe	AHowe@washoeschools.net
Open	Jamie Schocko	JSchocko@washoeschools.net
Open	Joseph Pazar	JPazar@washoeschools.net
Open	Amanda Schlatter	ASchlatter@washoeschools.net
Open	MICHAEL DIXON	MDixon@washoeschools.net
Open	Ryan Doetch-Youngblood	rdoetch@washoeschools.net
Open	Jennifer Dahlen	Jennifer.Dahlen@WashoeSchools.net
Open	Melissa Sullivan	MSullivan@washoeschools.net
Open	Colleen Winter	CWinter@washoeschools.net
Open	Jason Shipman	jshipman@washoeschools.net
Open	Joshua Reddig	JReddig@washoeschools.net
Open	Jennifer Hodges	JHodges@washoeschools.net
Open	Kim Polson	KPolson@washoeschools.net
Open	Heather Curtis	HCurtis@washoeschools.net
Open	Kristen Conway	KConway@washoeschools.net
Open	Angie Bryan	abryan@washoeschools.net
Open	Lisa Love	LLove@washoeschools.net
Open	SUSAN NOVELLI	SNovelli@washoeschools.net
Open	Brynn Hall	Brynn.Hall@washoeschools.net
Open	Derek Cordell	DCordell@washoeschools.net
Open	Ashley Mattick	Ashley.Mattick@WashoeSchools.net
Open	Monique Madrid-Luankaw	MMadrid@washoeschools.net
Open	Jake Chapin	Jake.Chapin@washoeschools.net
Open	Courtney Sego	CSego@washoeschools.net
Open	Allison Fannin	AFannin@washoeschools.net
Open	Eric Rogers	Eric.Rogers@washoeschools.net
Open	Elliot Grothe	EGrothe@WashoeSchools.net
Open	David Prell	David.Prell@WashoeSchools.net
Open	Chantal Lee	Chantal.Lee@washoeschools.net
Open	HEIDI GAVRILLES	HGavrilles@washoeschools.net
Open	Susan Adams	Susan.Adams@WashoeSchools.net
Open	Jonna Aucoin	jaucoin@washoeschools.net
Open	Sarah Zabel	Sarah.Zabel@washoeschools.net
Open	Nikki Capovilla	NCapovilla@washoeschools.net

Open	Samantha Shoolroy	SShoolroy@washoeschools.net
Open	Carrie Zabel	CZabel@washoeschools.net
Open	Sara Timmons	STimmons@washoeschools.net
Open	Jeana Miller	JeMiller@washoeschools.net
Open	Courtney Lean	CLean@washoeschools.net
Open	Shannon Ramacciotti	SRamacciotti@washoeschools.net
Open	Kristina Walker	KPWalker@washoeschools.net
Open	John Stern	JStern@washoeschools.net
Open	Kate Austill	kaustill@washoeschools.net
Open	Jill Dickey	Jill.Dickey@washoeschools.net
Open	Colbee Riordan	CRiordan@washoeschools.net
Open	Mindi Hammill	Mindy.Hammill@washoeschools.net
Open	Daniel Kirk	DaKirk@washoeschools.net
Open	Michelle Will	MWill@washoeschools.net
Open	Amanda Stulock	ASTulock@washoeschools.net
Open	Mari Riggs	mriggs@washoeschools.net
Open	April Coldani	April.Coldani@WashoeSchools.net
Open	Erin Dawson	EDawson@WashoeSchools.net
Open	Gladis Diaz	GDiaz@washoeschools.net
Open	Rebecca Bruemmer	RBruemmer@washoeschools.net
Open	Kelly Humphreys	KHumphreys@baileycharter.org
Open	Ahmet Ciftci	aciftci@coralacademy.org
Open	Eyup Ozturk	eozturk@coralacademy.org
Open	Jenny Hunt	jhunt@mariposaacademy.net
Open	Jonas Schenzel	jonas@hdmsreno.com
Open	Michael Martindale	MMartindale@washoeschools.net
Open	ELIAN GILBERT	EGilbert@washoeschools.net
Open	Amanda Lobkowicz	Amanda.Lobkowicz@WashoeSchools.net
Open	Lucy Dugan	LMDUGAN@WashoeSchools.net
Open	Dana Robert	DRobert@WashoeSchools.net
Open	Sarah Peterson	SEPeterson@washoeschools.net
Open	Jaime Bowers	JBowers@washoeschools.net
Open	Daniel Lediard	DLediard@washoeschools.net
Open	Kevin Arnold	KArnold@washoeschools.net
Open	DAVID HARTSHORN	DHartshorn@washoeschools.net

Open	Murat Kurt	MKURT@CORALACADEMY.ORG
Open	Kendra Carlsen	kendra.carlsen@washoeschools.net
Open	Dustin Beil	DBeil@WashoeSchools.net
Open	Mandie Sheridan	MLSheridan@washoeschools.net
Open	Colleen Quayle	CQuayle@coralacademy.org
Open	Jill Bayliss	JBayliss@washoeschools.net
Open	CHERYL GARLOCK	CGARLOCK@CORALACADEMY.ORG
Open	Catherine Phillips	CAPhillips@WashoeSchools.net
Open	Kimberly Crowley	KACrowley@washoeschools.net
Open	David Kitchin	David.Kitchin@washoeschools.net
Open	MIKE NAKASHIMA	MNakashima@washoeschools.net
Open	Cynthia Waddell	CWaddell@washoeschools.net
Open	Tristan McElhany	TMcelhany@washoeschools.net
Open	Josh Rosenbloom	JRosenbloom@washoeschools.net
Open	Leah Ramsey	Leah.Ramsey@WashoeSchools.net
Open	Freeman Holbrook	fholbrook@washoeschools.net
Open	R. JAY SALTER	RJSalter@washoeschools.net
Open	Michael Bradley	Michael.Bradley@WashoeSchools.net
Open	Mike Gifford	mgifford@washoeschools.net
Open	Stacey Black	STBlack@washoeschools.net
Open	Tierney Cahill	TCahill@washoeschools.net
Open	Cristina Oronoz	Cristina.Ornoz@washoeschools.net
Open	Kimberly Regan	kregan@snacs.org
Open	Sean Hall	SHall@washoeschools.net
Open	Tomas Macaluso	TMacaluso@washoeschools.net
Open	Adam Nicely	anicely@acehighschool.org
Open	Darvel Bell	dsbell@washoeschools.net
Open	Adam Kahn	adam@encompassacademy.org
Open	Jason Mattick	JMattick@washoeschools.net
Open	TINA SPRINGMEYER	tspringmeyer@washoeschools.net
Open	Mandie Sheridan	MLSheridan@washoeschools.net
Open	Denise DuFrene	DDuFrene@washoeschools.net
Open	Claudia Bessette-Goetz	CBessette@WashoeSchools.net
Open	Steven Constantino	SConstantino@washoeschools.net
Open	Trisha Lozano	tlozano@washoeschools.net

Open	Cristina Oronoz	Cristina.Oronoz@washoeschools.net
Open	Jody Rogers	JRogers@washoeschools.net
Open	Timothy Moser	tim.moser@wpcnvadmin.com
Open	Robert Bischoff	robert.bischoff@wpcnvadmin.com
Open	Kenna Hall	kenna.hall@wpcnvadmin.com
Open	Robert Bischoff	robert.bischoff@wpcnvadmin.com
Open	Dr. Jerri Lynn Williams-Harper	jerri.williams@wpcnvadmin.com
Open	Kristina Ernest	kristina.ernest@wpcnvadmin.com
Open	Kelly Sturgeon	kelly.sturgeon@wpcnvadmin.com
Open	Timothy Moser	tim.moser@wpcnvadmin.com
Open	Curtis Nielson	curtis.nielson@wpcnvadmin.com
Open	Kenna Hall	kenna.hall@wpcnvadmin.com
Open	Jerri-Lynn Williams-Harper	jerri.williams@wpcnvadmin.com
Open	Adam Young	
Open	Jeremy Christensen	jchristensen@freedomclassical.org
Open	Brian Meadows	Brian.Meadows@legacytraditional.org
Open	Tony Davis	Tony.Davis@legacytraditional.org
Open	Jessica Alanano	Jessica.Alanano@legacytraditional.org
Open	Ignacio Prado	director@futuroacademy.org
Open	Gia Maraccini	Gia.Maraccini@maternnv.org
Open		
Open		
Open		
Open		
Open		
Open		
Open		
Open		
Open		
Open		
Open		
Open		
Open		
Open	Lawrence Weekly	
Open	Dan Triana	dan.triana@slamnv.org

Open	Benjamin Salkowe	ben.salkowe@equipoacademy.org
Open	Renee Fairless	renee.fairless@materlv.org
Open	Danielle Ranney	danielle.ranney@materlv.org
Open	Olivia Carbajal	olivia.carbajal@materlv.org
Open	Amy Gronna	Amy.Gronna@materlv.org
Open	Renee Fairless	Renee.Fairless@materlv.org
Open	Sabrina Carrington Jackie Jackson	scarrington@amplus.academy
Open	Lisa Cates	lcates@amplus.academy
Open	Ronald Fick	ronald.fick@fcalv.net
Open	Bryon Richardson	bryon.richardson@lanv.org
Open	Amanda Campbell	acampbell@elylearningbridge.org
Open	Bethany Farmer	bethany.farmer@doralacademynv.org
Open	Kelly Gerdes	kelly.gerdes@doralacademynv.org
Open	Danielle McDowell, Steve Piccininni	Danielle.McDowell@doralacademynv.org
Open	Amy Smith	amyn.smith@doralacademynv.org
Open	Julianna Turley	julianna.turley@doralacademynv.org
Open	Andrea Morency	dr.andi@academyoflit.org
Open	Wendy Shirey	wendy.shirey@pinecrestnv.org
Open	Bryan Rudden	bryan.rudden@pinecrestnv.org
Open	Michael O'Dowd	michael.odowd@pinecrestnv.org
Open	Jon Haskel	jon.haskel@pinecrestnv.org
Open	Lisa Satory	lisa.satory@pinecrestnv.org
Open	Bryan Rudden	bryan.rudden@pinecrestnv.org
Open	Jessica Medina	jessica.medina@pinecrestnv.org
Open	Yvette Simmons	yvette.simmons@salv.org
Open	Jessica Scobell	jessica.scobell@salv.org
Open	Cesar Tiu	Cesar.Tiu@salv.org
Open	Lee Esplin	Lee.Esplin@salv.org
Open	David Fossett	David.Fossett@salv.org
Open	Shannon Manning	shannon.manning@salv.org
Open	Kate Lackey	kate.lackey@salv.org
Open	Abbe Mattson	amattson@ekacademy.org
Open	Friederike Opalinski	fopalinski@dcslv.org
Open	Denise Koch	dkoch@dcslv.org
Open	Shambrion Treadwell	streadwell@dobeartsacademy.org

Open	Janice Henry	janice.henry@rdacharter.org
Open	Tori Sleight	tsleight@oasisacademyfallon.us
Open	Angela Orr	Angela.Orr@doralnnv.org
Open	Bruce Congleton	bruce.congleton@deltaacademylv.com
Open	Ashley Perkins	aperkins@eiaanv.net
Open	Connie Malin	connie_malin@iicsn.org
Open	Connie Malin	connie_malin@iicsn.org
Open	Janelle Veith	j.veith@questlv.com
Open	Nichole Shaffer	nichole.shaffer@imaginemountainview.org
Open	Kristen Guthrie	kristen.guthrie@futuresedgeacademy.org
Open	Lewis Perlin	lperlin@alpineacademy.net
Open	Tim Lorenz	tlorenz@odysseyk12.org
Open	Marlo Tsuchiyama	ms.marlo@silversandsmcs.org
Open	Chet George	cgeorge@dcsf.nv.gov
Open	Christa Fialkiewicz	cfialkiewicz@nevadastatehs.com
Open	Christa Fialkiewicz	cfialkiewicz@nevadastatehs.com
Open	Christa Fialkiewicz	cfialkiewicz@nevadastatehs.com
Open	Christa Fialkiewicz	cfialkiewicz@nevadastatehs.com
Open	Christa Fialkiewicz	cfialkiewicz@nevadastatehs.com
Open	Christa Fialkiewicz	cfialkiewicz@nevadastatehs.com
Open	Christa Fialkiewicz	cfialkiewicz@nevadastatehs.com
Open	Colleen Harsin	charsin@davidsonacademy.unr.edu
Open	Daniel Cisar	dacisar@nca.connectionsacademy.org
Open	Yolanda Hamilton	yolanda.hamilton@nvvirtual.org
Open	Kayla Davis	kdavis@coralacademylv.org
Open	Miadora Nelson	mnelson@coralacademylv.org
Open	Adem Akgedik	aakgedik@coralacademylv.org
Open	Zack Ocel	zocel@coralacademylv.org
Open	Ismail Kocabiyik	ikocabiyik@coralacademylv.org
Open	Tiffany Bailey	tbailey@coralacademylv.org
Open	Emrullah Eraslan	eeraslan@coralacademylv.org
Open	Andrea Damore	andrea.damore@banv.org
Open	Mike Taack	mike@wylees.org
Open	Candi Wadsworth	candi.wadsworth@snvtradeshighschool.org

Open	Vincent Medina	vincent.medina@thrivepointnevada.com
Open	Benjamin Feinstein	drbfeinstein@vegasvistaacademy.org
Open	Brandolyn Thran	bthran@ncaelko.org
Open	Justin Brecht	jbrecht@nevadarise.org
Open	Christa Fialkiewicz	cfialkiewicz@nevadastatehs.com
Open	Carey Roybal-Benson	carey@signatureprep.org
Open	Jami Austin	jami.austin@pinecrestnnv.org
Open	Alexandra Taylor	alexandria.taylor@explore.academy
Open	Richard Santigate	richard.santigate@civicnv.org
Open	Keturah Draper	kdraper@ywlalv.org
Open	Miriam Benitez	mbenitez@clvstrongstartes.org
Open	Andrea Tee	atee@amsnellis.org
Open	Eve Breier	ebreier@kesheracademy.org

Test Coordinator First Name	Test Coordinator Last Name	School Test Coordinator Phone
Linnell	Cramer	7754235184
Brad	Barton	7754233159
Kimi	Melendy	7754231999
Shawn	Purrell	7754281996
Heather	Alves	7754237701
Tim	Spencer	7754232181
Chantelle	Redner	7754231191
Shawna	Quenneville	7027992510
Samantha	Schuller	7027992570
Lori	Schaeffer	7027993200
Ana	Tervo	7027995888
Chelsea	Starr	7027992680
Leanna	Mackelprang	7027995915
Lourdes	Pearson	7027994585
Dezzaray	Genovese	7027991252
Aimee	Levy	7027991420
Candace	Feller	7027992525
Elizabeth	Stuflick	7027990220
Erin	Monterastelli	7027998170
LaQuisha	Johnson	7027994920
Cheryl	Lopez	7027991360
Kelly	Slear	7027994640
Wanda	Colon-Diaz	7027997100
Lori	Lynch	7027995776
Christine	Manjarrez	7027992274
Kristen	Davis	7027992140
Eugene	Toyama	7027996882
Michele Nicole Schuebel		7027996608
Matthew	Okada	7027991890
Jennifer	Speakman	7027996600
Jennifer	Stiles	7027995702
Ashley	Martin	7027992120
Joan	Howard	7027991766
Christopher	Isle	7027997500

Tisha	Jones	7027993120
Bridget	Mecham	7027998090
Travis	Davie	7027991805
Tammy	Brown	7027993878
Timothy	Granger	7027997510
Michelle	John	7027995890
Danielle	Jordan	7027996840
Lynette	Shipman	7027992201
Shannon	Williamson	7027991380
Mariah	Mears	7027994501
Debra	Stancliff	7028754226
Christopher	Welch	7028725438
Tracy	Echeverria	7022971224
Jessica	Nuckoles	7027997390
Jessica	Robbins	7027994600
Sonia	Etelis	7027995990
Domonique	Powell	7027995700
Lindsey	Kepner	7027994390
Melanie	McCraney	7027994530
Andrea	Hill	7027998060
Brian	Flynn	7027998680
Christina	Bass	7027994350
Marianne	Ekenstam	7028642444
Tricia	McDermott	7027998820
Kang	Linares	7027994970
Kelly	Klassen	7027998360
Kelley	Stone	7027994680
Melissa	Dawkins	7027994890
Blair	Rodrigues	7027998730
Beth	Ralston	7027998160
Ashley	Zinovitch	7027995720
James	Mori	7027994320
Hannibal	Nisperos	7027994370
Melanie	Blanco	7027998780
Andrea	Heinlen	7027995730

Amanda	Hemenway	7027998760
Shawana	King	7027997380
Brittany	Doran	7027998860
Malori	Hewitt	7027995690
Jennifer	Renville	7027998800
Melissa	Mingo	7027994690
Rachelle	Tetlow	7027994660
Jordan	Tanner	7027994330
Jose	Hernandez	7027998140
Jason	Schrock	7027998260
Christine	Clayman	7027995750
Danielle	Fishpaw	7027994440
Aaron	Walker	7027990740
Leah	Ann Ferrario	7027998380
Sara	Young	7027994380
Bridgette	Nygard	7027995760
Sonja	Clark	7027990600
Natalie	Newcombe	7027994930
Stacy	Limoncelli-Moses	7027994450
Shawna	Yelton	7027990500
Athena	Garrison	7027990620
Arlene	Andrade	7027991460
Lindy	Specht	7027991750
Kristin	Chase	7027991320
Juanita	Frasier	7027994580
Amanda	Skrogstad	7027991860
Rick	Crandall-Malone	7027991550
Rikki	Wiggs	7027990540
Alicia	Norman	7027991700
Kelley	Viskovich	7027991270
Michele	Keener	7027996050
Michael	Dobbyn	7027991350
Summer	Whitney	7023461900
Dana	Mays	7027993450
Jill	Simonini	7027993150

Bertrand	Christophe	7027993550
Carlene	Hardin	7027993420
Stephanie	Garni	7027991730
Heather	Gumina	7027992180
Angie	Niemann	7027991330
Stephanie	Hernandez	7027996000
Kathleen	Starling	7027996030
Joseph	Kielminski	7027996300
Traci	McLaughlin	7027992200
Nicole	Lawrence	7027996650
Kelly	Cano	7027996630
Christine	Self	7027996690
Kathryn	Bell	7027996870
Janet	Diaz	7027993750
Jodi	Janiga	7027996860
Tiffany	Amaro	7027997040
Jandelle	Blackway	7027992590
Karen	Sawyer	7027997250
Tamara	Martinez	7027990690
Erin	Erdman	7027996899
Victoria	Watkis	7027997260
Jennifer	Gomez Lopez	7027990570
Blair	Lewis-Williams	7027991402
Allison	Puana	7027991430
Evan	Billings	7027992520
Nicole	Bryan	7027996810
James	Harenberg	7027993401
Lisa	Dalton	7027991891
Tori	Goldstein	7027992504
Argelia	Bell	7027994701
Patrick	White	7027992550
Chris	Sparrow	7027991920
Janet	Perez	7027991240
Michael	Blume	7027991899
Heather	Lenz	7027992100

Jill	Fisher	7027991770
Nicole	Noble	7027993430
Shiobhan	Henderson	7027993870
Michelle	Basolo	7027995701
Michelle	Pallares	7027994780
Constance	May	7027994740
Michelee	Crawford	7027997159
Opal (Lynn)	Ivey	7027997169
Dawn	Gruner	7027997890
Merrick	Murray	7027994730
Sarah	Donald	7027994205
Janel	Gellens	7027994200
Anna	Slighting	7027997123
Brynn	Dessormeau	7027997896
Cullen	Skyles	7027994720
Zakiya	Sutton	7027997310
Debby	Korder	7027994900
Amber	Radjeski	7027997780
Nathan	Anderson	7027997401
Reagan	Raham	7027997904
Marian	Carter	7027997139
Donald	Bacon	7027994770
Michelle	Hervey	7027997113
Julie	Russell	7027997710
Kailey	Baskin	7027995540
Eugeena	Horner	7027997133
Heather	Bergdoll	7027994910
Darius	Hogans	7027994760
Nita	Leicht	7027997103
Sherence	Sathekge	7027994750
Delilah	Krasch	7027997479
David	Navarette	7027997350
Rachel	Dupris	7027996892
Matt	Landal	7027994185
DiSheen	Smith	7027995660

Deanna	Bottrell	7027994800
Amanda	Lush	7027997149
Sarah	Silva	7027994223
Keon	Pierre	7027995910
Paola	Zepher	7027995530
Melodie	Garcia	7027994233
Cristy	Luke	7027995550
Adrienne	Dragon	7027997912
Merideth	Wallace	7027997179
Alicia	Tommela	7027994790
La Tonya	Juniel	7027994213
Maureen	Clowers	7027995960
Michelle	Wright	7027997095
Adam	Bellamy	7027994239
Shannon	Brown	7027997700
Wendy	Hale	7027998930
Tracy	Echeverria	7027998280
Stacy	Hawken	7027998940
Dana	Cervantes	7027990932
Michelle	Caligone	7027996200
Melissa	Leicht	7027998950
Vanessa	Moreno-Solis	7023465761
Julie	Causey	7027997790
Vera	Jordan	7027997720
Edwin	Evans	7027995650
Corianne	Guerin	7027998600
Christina	Mehl-Smith	7027997360
Victoria	Ellington	7027997740
Christine	Casas	7027997750
Andrew	Schwab	7027995930
Tiffany	Orbon	7027994300
Alexis	Olige	7027997770
Terri	Johnson	7027995940
Christine	Savino	7027997320
Joseph	Fernandez	7027997730

Melissa	Dalpee	7027995920
Paige	Karetny	7027997456
Corinna	Soliwoda	7027994646
Jenny	Rash	7027992298
Amy	Johnson	7027991660
Jilly	Hauritz	7027998830
Hazel J.	Alfaro	7027997330
Jessica	Knudson	7027998920
Nicole	Leighton	7027997760
Liliana	Kulaszewski	7027995950
Veronica	Zinovitch	7023983233
Stacey	Burgess	7027992220
Mary	McNeal	7027993800
Kelly	Leong	7027993270
Sharla	Meyer	7027996077
Angie	Shepard	7027993700
Tiffany	Ferguson	7027996710
Kim	Crowe	7027996720
Melanie	Danzeisen	7027992230
Patricia	Reuter	7027991120
Mashelia	Moore	7027994500
Stacy	Schaumburg	7027990935
Jonathan	Moss	7022983378
Lakeisha	Myers	7027994990
Sarah	Udy	7027997272
Malisa	Riggle	7027994777
David	Bell	7027998181
David	Copenbarger	7027998990
Darla	Richards	7027997788
Rachel	Petrimoulx	7027991830
Dulce	Hernandez	7027997280
Joshua	Covert	7027994245
Christine	Notareschi-Rinard	7027994260
Golda	Gilliam	7027995880
Cassandra	Cruz	7027997080

Sherri	Schrieber	7027994550
Heather	Bennett-Willis	7027997185
Johnson,	Rosanna	7027995558
Nick	Christiansen	7027997470
Takisha	Davis-Woods	7027994700
Marianne	Ramos	7027997922
Treemonisha	Addison	7027995573
Eliza	Perez	7027998080
Loreen	Garcia	7027997660
Kelli	Han	7027995600
Barbara	Pangelinan	7027995900
Brian	Todd	7027998290
Laura	Traymany	7027998900
Stacy	Schaumburg	7027990935
Brad	Hockett	7022981996
Eric	Videau	7027997340
Dana	Dyer	7027994480
Katja	Hermes	7027990920
LaJuana	Jackson-Gates	7027994860
April	Barr	7027990777
Derek	Krallman	7027994460
Jeff	Dalton	7027995980
Kim	Bunker	7023978610
Tisha	Jones	7027993120
Silvia	Mendoza-Stout	7027994620
Catherine	Evans	7027993220
Maylin	Lara	7027993400
J. Huston	Todd	7027992240
Jacob	Bendixen	7027992400
Dana	Cervantes	7027990932
Nicole	Doering	7027992540
Chris	Miller	7027992260
Michelle	Saitta	7027996040
Danielle	Atkinson	7027994699
Shannon	Koss	7027997020

Shirley	Serrano Pedraza	7027993670
Terri	Rodriguez	7027992290
Randee	Greco	7027993880
Shira	Wise	7027993240
Jeanine	Roser	7027991900
Jaclyn	Martin	7027996692
Melissa	Carrizzo	7027991340
Stephen	Walters	7023463250
Shaunte'e	Wilson-Knox	7027993160
Zach	Stork	7027993020
Brian	Levanger	7027993460
Jennifer	Mattox	7027991305
Brently	Garbutt	7027992005
Kenny	Robinson	7027994811
Greg	Sanders	7027997001
Rori	Romero	7027996801
Brittany	Wadas	7027994560
Shirley	Cunningham	7027996850
Jennifer	Wiggins	7027992560
Marian	Carter	7027997139
Amber	Foy	7027995800
Dubb	Mapp	7027990180
Tracy	Pacheco	7027997000
Brent	Fujino	7027995450
Starra	Pollard	7027994080
Gayle	Miller	7027998000
Stacey	White	7027998880
Sergio	Lopez	7027997580
Antionette	Odediran	7027997200
Janelle	Bolino	7027994000
Christopher	Isle	7027997500
Kenya	Neal	7027994400
Maria	Konrad	7027994830
David	Hawley	7027990950
Amy	Forrest	7027995850

Jenny	Valdez	7027997800
Sharon	Ruesch	7027997870
Bianca	Lutchen	7027995790
Stefanie	Machin	7026514070
Stefanie	Machin	7026515030
Lisa	Louw	7027990432
Daniel	Liles	7027991450
Stefanie	Machin	7026513080
Stephanie	Jordan	7027996699
Shelby	Jones	7027992270
Pingxi	Hodrosky	7027991870
Mildred	Zamorano-Perry	7027996830
Olivia	Cooper	7027992580
Erika	Benedict	7027994710
Adonai	Shiman	7027995766
Alex	Alger	7027997207
Devyn	Horst	7027994340
Anna	Sumsion	7027992250
Alexis	Sharp	7027998200
Mitchell	Ozaki	7023972611
Brian	Poole	7023462780
Dana	Cervantes	7027990932
Jessica	Maleskey	7027993440
Dana	Perry	7027993500
James	Charlton	7027992196
Kristen	Cutitta	7027996820
Trisha	Davenport	7027996800
Tasha	Estes	7027996660
Kathy	Price	7027991777
Kelly	Slear	7027994640
Katie	Kelly	7027996881
Johnathan	Carter	7027998888
Colleen	Moriarty-Ramirez	7027996852
Colleen	Moriarty-Ramirez	7027996852
Sean	Marshall	7027990250

Roxane	Thomas	7027991720
Tracey	Clark	7029529773
Gina	Piccolo	7027991623
Nicole	Delgado	7027991720
Melissa	Robertson	7027991111
Maria	Konrad	7027994830
Kenya	Neal	7027994400
Vanessa	Paniagua	7027992196
Starra	Pollard	7027994080
Janelle	Bolino	7027994000
Rick	Fuller	7027995588
Amie	Renegar	7027997938
Gina	Piccolo	7027991623
Joshua	Katz	7024555023
Rebecca	VanDePol	7027995631
Rebecca	VanDePol	7027995631
Leilani	Shive	7027990275
Amy	Miller	7027998150
Oscar	Padilla	7027998850
Kamille	Bryner	7027996370
Rebecca	VanDePol	7027995631
Rebecca	VanDePol	7027995631
Tawanda	Butler	7027992070
Stacey	Johnston	7027996380
DeSoto	Dickson	7027996610
Amie	Renegar	7027997938
Gina	Piccolo	7027991623
Michael	Rolands	7252166824
Amber	D'Alliegro	7027998650
Margaret	Ann Froby	7252166581
Leilani	Shive	7252166150
Lonna	Kelly-Ibarra	7027996240
Michael	Rolands	7252166824
Angela	Nickels	7027997880

Amy	Manning	7027993002
Gina	Piccolo	7027991623
Veronica	Griffith	7757825117
Sean	Ryan	7755884574
Heather	Duncan	7752673267
Blaine	Spires	7752652222
Jason	Reid	7752673622
Andrew	Fromdahl	7757825510
Greg	Thetford	7757822265
Amy	Carter	7752656100
Michael	Rechs	7757825136
Alicia	Braaksma	7755882446
Stormy	Herald	7752655433
Stormy	Herald	7723921475
Stormy	Herald	7753921480
Mike	Rechs	7757825136
Stormy	Herald	7753921475
Amy	Kidman-Delaney	7752655262
Jeffrey	Revier	7757387255
Stormi	McCarthy	7757552375
Patrick	DiSpirito	7756643100
Jessica	Harris	7757384711
Angela	Silva	7757523477
Bobby	Steensen	7757533667
Sean	Stanton	7757387161
Jeffrey	Revier	7757387255
Thomas	Cunningham	7757383731
Mauro	Lobato	7757546317
Lynn	Manning John	7757573400
Angela	Silva	7757523837
Patrick	DiSpirito	7756643100
Cynthia	Etchemendy	7757381844
Chrissie	Blanchard	7757536881
Jessica	Harris	7757384711

[illegible]

Noel	Morton	7756238107
Noel	Morton	7756236107
Noel	Morton	7756238107
Diana	Padua	7756238277
Jacquie	Buchel	7756358114
Jacquie	Buchel	7756358114
Jacquie	Buchel	7756358114
Jacquie	Buchel	7756358114
Jaqueline	Buchel	
Mike	Sparrow	7757253351
Doug	Peterson	7757263772
Raymond	Wadsworth	7757284446
Stephanie	Vincent	7759625832
Michael	Roth	7757284655
Brooke	Foremaster	7757253321
Sharon	Dirks	7757284481
Brooke	Foremaster	7757253321
MaCall	Barnes	7757268250
Cherry	Florence	7757288019
Cherry	Florence	7757288019
Chase	Woodford	7752466262
Rich	Fortier	7754636844
Jaime	Henderson	7755753420
Erin	Korf	7755775060
Kent	Jones	7755753332
Kevin	Kranjcec	7752466250
Virginia	Richardson	7755753414
Corinne	Burns	7752466270
Rachel	Kuhn	7752466170
Scott	Gillespie	7754636833
Reema	Pulsifer	7755753390
Jed	Marciniak	7755775050
Steve	Henderson	7755751575
Ryan	Cross	7755753400

Stephanie	Coplan	7754652332
Kathy	Bomba-Edgerton	7754636822
Julie	Bumgardner	7752466240
Amber	Cross	7755775071
Amber	Cross	7755775071
James	Ruff	7755753409
Rachel	Stewart	7754636800
Chanen	Cross	7755775128
Erika	Sterling	7759452403
Erika	Sterling	7759452403
Erika	Sterling	7759452403
Erika	Sterling	7759452403
Erika	Sterling	7759452403
Samantha	Moore	7757275252
Thaddeus	Wind	7753772236
Holly	Riggs	7752852692
Amanda	Arceo	7753725324
Sylvia	DeMasi	7757276619
Andrew	Jones	7755532902
Timothy	Wombaker	7754826644
Elizabeth	Gilligan	7757277892
Jared	Peruch	7757514688
Greg	Bailey	7757514060
April	Sutton	7757275546
Andrew	Jones	7755532902
Timothy	Wombaker	7754826644
Thaddeus	Wind	7753772690
Holly	Riggs	7752852692
Amanda	Arceo	7753725324
Andrew	Jones	7755532595
Holly	Riggs	7752852692
Timothy	Wombaker	7754826644
Desiree	Veloz	7757277737
Thaddeus	Wind	7753772690
Holly	Riggs	7757516822

Holly	Riggs	7757516822
Holly	Riggs	7757516822
Holly	Riggs	7757516822
Shannon	Slamon	7752832404
Robert	Chambers	7752831352
Nicole	Whitsett	7752831403
Jeff	Hurzel	7752831204
Ryan	Icanberry	7752832204
Nathan	Brigham	7752831104
Sara	Casacca	7752831006
Allison	Cooper	7758879500
JEREMY	LEWIS	7752832805
Lois	Linehan	7752832612
SUE	MOULDEN	7752831622
Eva	Nelson	7752732176
Eva	Nelson	7752732176
Eva	Nelson	7752732625
Eva	Nelson	7752732625
Eva	Nelson	7752732625
Shaun	Terry	
Karen	Staffen	7758470977
Karen	Staffen	7758470977
Karen	Staffen	7758470977
Karen	Staffen	7758470977
Kevin	Sady	7756892500
Marcus	Culpepper	7756892540
JESSICA	WILSON	7757465850
Ryan	Smith	7753335190
Barbara	Surritte-Barker	7757465830
AMANDA	MCWILLIAMS	7753335040
RYAN	SMITH	7756892520
MARY	CULPEPPER	7753335140
KRISTINA	MARTIN	7757465820
JEFF	BATAVIA	7757467440
RICHARD	MARES	7753335030

HEATHER	THAXTON	7758506212
Amy	Howe	7757465840
JAMIE	SCHOCKO	7753535750
Joseph	Pazar	7753335180
Amanda	Schlatter	7753335000
MICHAEL	DIXON	7756892560
RYAN	DOETCH-YOUNGBLOOD	7756775480
Jennifer	Dahlen	7753335090
MELISSA	SULLIVAN	7753535760
COLLEEN	WINTER	7753535580
Jason	Shipman	7753535510
JOSHUA	REDDIG	7753535530
Jennifer	Hodges	7753535720
KIM	POLSON	7753535540
HEATHER	CURTIS	7753535570
KRISTEN	CONWAY	7753535590
ANGIE	BRYAN	7758515600
LISA	LOVE	7756892510
SUSAN	NOVELLI	7753335080
BRYNN	HALL	7756775460
DEREK	CORDELL	7758490255
Ashley	Mattick	7756744420
Monique	Madrid-Luankaw	7753458100
JAKE	CHAPIN	7753511902
COURTNEY	SEGO	7753535730
ALLISON	FANNIN	7753535520
ERIC	ROGERS	7756744400
Elliot	Grothe	7754257755
DAVID	PRELL	7756265257
CHANTAL	LEE	7758526570
HEIDI	GAVRILLES	7756260062
SUSAN	ADAMS	7756773800
Jonna	Aucoin	7758515444
Sarah	Zabel	7758324250
Nikki	Capovilla	7756775440

SAMANTHA	SHOOLROY	7758515620
Carrie	Zabel	7756892530
SARA	TIMMONS	7756265200
JEANA	MILLER	7756775410
COURTNEY	LEAN	7756892600
Shannon	Ramacciotti	7758573150
KRISTINA	WALKER	7756775400
JOHN	STERN	7757465800
KATE	AUSTILL	7754257700
JILL	DICKEY	7756744430
COLBEE	RIORDAN	7753535507
MINDY	HAMMILL	7756775444
DANIEL	KIRK	7754257710
MICHELLE	WILL	7757465810
AMANDA	STULOCK	7756265250
MARI	RIGGS	7756892626
APRIL	COLDANI	7753535950
Erin	Dawson	7758517095
GLADIS	DIAZ	7756744444
Rebecca	Bruemmer	7754257722
KELLY	HUMPHREYS	7753236767
Ahmet	Ciftci	7753579122
Eyup	Ozturk	7754181115
JENNY	HUNT	7758264040
JONAS	SCHENZEL	7756242800
Michael	Martindale	7757465860
ELIAN	GILBERT	7753335330
AMANDA	LOBKOWICZ	7753335160
Lucy	Dugan	7753335130
Dana	Robert	7753535740
SARAH	PETERSON	7753535770
JAIME	BOWERS	7756775420
DANIEL	LEDIARD	7758324220
KEVIN	ARNOLD	7757465870
DAVID	HARTSHORN	7753535990

MURAT	KURT	7758294601
KENDRA	CARLSEN	7758526700
Dustin	Beil	7754257777
Mandie	Sheridan	7756775433
COLLEEN	QUAYLE	7753220274
JILL	BAYLISS	7756260060
CHERYL	GARLOCK	7753232332
Catherine	Phillips	7756744915
KIMBERLY	CROWLEY	7758515629
DAVID	KITCHIN	7753213160
MIKE	NAKASHIMA	7753335050
CYNTHIA	WADDELL	7753535550
TRISTAN	MCELHANY	7753335300
JOSH	ROSENBLOOM	7753535700
Leah	Ramsey	7758573181
Freeman	Holbrook	7757465880
JAY	SALTER	7758515630
Michael	Bradley	7753335150
Mike	Gifford	
STACEY	BLACK	7755572326
TIERNEY	CAHILL	7758324260
CRISTINA	ORONOZ	7756747660
KIMBERLY	REGAN	7756774500
Sean	Hall	7754257733
TOMAS	MACALUSO	7756775499
Adam	Nicely	7753243900
DARVEL	BELL	7758515656
ADAM	KAHN	7753225566
JASON	MATTICK	7753273920
Tina Springmeyer		7753270675
TINA	SPRINGMEYER	7753270675
DENISE	DUFRENE	7758515650
CLAUDIA	BESSETTE-GOETZ	7753377560
STEVEN	CONSTANTINO	7753379939
Trisha	Lozano	7758573181

CRISTINA	ORONoz	7753536900
Jody	Rogers	7753270685
Tim	Moser	7752385200
Robert	Bischoff	7752932052
Kenna	Hall	7752894846
Robert	Bischoff	7752357722
Jerri	Williams-Harper	7752894811
Kristina	Ernest	7752894811
Kelly	Sturgeon	7752894811
Tim	Moser	7752385200
Curtis	Nielson	7752892999
Kenna	Hall	7752892999
Anthony	Pucci	7025331896
Jaime	Cornell	7023420880
Angie	Green	7028462216
Alia	Rothstein	7026371776
Cindi	Rivera	7025469139
Gia	Maraccini	7754708950
Shannon	Hamilton	7023162410
Erin	Kipp	7024735735

Ben	Salkowe	7029070432
Karli	Casto	7257262626
Danielle	Ranney	7023707891
Amy	Rivera	7024852400
Anissa	Hilyard	7024788318
Danielle	Ranney	7024629361
Susan	McGuan	7029706800
Susan	McGuan	7029706800
Daniel	Bonkobara	7029988368
Ryan	Rasar	7023501472
Milo	Jury	7752938009
Erin	Bedich	7029607500
Kristal	Urso	7029014950
Erin	Bedich	7025347990
Erin	Bedich	7027766491
Erin	Bedich	7029164320
Andrea	Morency	7757374084
Christine	Garvin	7024629700
Christine	Garvin	7024629700
Christine	Garvin	7024629700
Christine	Garvin	7024629700
Christine	Garvin	7024629700
Christine	Garvin	7024626260
Christine	Garvin	7024629700
Christine	Garvin	7024629700
Crystal	Hampton	7026335616
Jennifer	Ludtke	7028264373
Cesar	Tiu	7026859150
Lee	Esplin	7024788888
Jennifer	Steele	7029980500
Morgan	Carrona	7029162327
Emeri	Rodriguez	7024892473
Abbe	Mattson	7028705032
Denise	Koch	7022400359
Denise	Koch	7022400359
Shambrion	Treadwell	7024201519

Nikisha	Bangerter	7026380222
Jami	Rowlett	7754235437
Nicolette	Smith	7754534239
Austin	Congleton	7023962252
Royelle	Mickelson	7757383422
Linda	Mazurkiewicz	7022164337
Linda	Mazurkiewicz	7022164337
Janelle	Veith	7026314751
Crystal	Gibson	7022530251
Kristen	Guthrie	7026362551
Lewis	Perlin	7753561166
Brad	Evans	7022570578
Sheila	Palombo	7025226220
Ashley	O'Connell	7757385907
Christa	Fialkiewicz	7029532600
Christa	Fialkiewicz	7029532600
Christa	Fialkiewicz	7029532600
Christa	Fialkiewicz	7029532600
Christa	Fialkiewicz	7029532600
Christa	Fialkiewicz	7029532600
Christa	Fialkiewicz	7029532600
Christa	Fialkiewicz	7029532600
Rebecca	Celler	7754467778
Taneil	Wood	5305624901
Jennifer	Okamura	7024071825
Julene	Ballard	7026854333
Rowena	Martin	7026435121
Autumn	Nourse	7027768800
Bethany	Mickey	7022698512
Deniz	Tarim	7024853410
Samantha	Sokolowski	7024899797
Annette	Martin	7026656998
Lola	Brooks	7027268600
Mike	Taack	7023234524
Candi	Wadsworth	7022442771

Vincent	Medina	7028448854
Benjamin	Feinstein	7023017983
Brandolyn	Thran	7758604300
Justin	Brecht	7023367060
Christa	Fialkiewicz	7029532600
Danielle	Strough	7028679711
Jami	Austin	7753761444
Melissa	Hernandez	7024836332
Karen	Tanaka	7024629653
Keturah	Draper	3525028132
Tino	Mora	7024630222
Andrea	Tee	7026036770

School Test Coordinator Phone Extension	NCES DistrictID	NCES School ID	Locale	School Level
	3200030	00005	10: Town - Remote	PK: PreK
	3200030	00004	10: Town - Remote	ES: Elementary School
	3200030	00021	10: Town - Remote	ES: Elementary School
	3200030	00431	10: Town - Remote	ES: Elementary School
	3200030	00003	10: Town - Remote	MS: Middle School
	3200030	00001	10: Town - Remote	HS: High School
	3200030	00868	10: Town - Remote	AD: Adult HS
4201	3200060	00946	08: Suburb - Large	ES: Elementary School
4201	3200060	00935	08: Suburb - Large	ES: Elementary School
4201	3200060	00933	08: Suburb - Large	ES: Elementary School
4201	3200060	00930	04: City - Large	ES: Elementary School
4203	3200060	00915	08: Suburb - Large	ES: Elementary School
4201	3200060	00916	03: City - Midsize	ES: Elementary School
4201	3200060	00927	04: City - Large	ES: Elementary School
4203	3200060	00874	08: Suburb - Large	ES: Elementary School
4201	3200060	00877	06: Rural - Fringe	ES: Elementary School
4201	3200060	00873	08: Suburb - Large	ES: Elementary School
4203	3200060	00875	06: Rural - Fringe	ES: Elementary School
4201	3200060	00876	08: Suburb - Large	ES: Elementary School
4203	3200060	00879	08: Suburb - Large	ES: Elementary School
4201	3200060	00872	08: Suburb - Large	ES: Elementary School
4200	3200060	00814	04: City - Large	OC: Other Combination
4203	3200060	00805	08: Suburb - Large	ES: Elementary School
4201	3200060	00804	04: City - Large	ES: Elementary School
4201	3200060	00816	06: Rural - Fringe	ES: Elementary School
4203	3200060	00801	08: Suburb - Large	ES: Elementary School
4027	3200060	00771	08: Suburb - Large	ES: Elementary School
4201	3200060	00786	04: City - Large	ES: Elementary School
4201	3200060	00806	08: Suburb - Large	ES: Elementary School
4201	3200060	00758	04: City - Large	ES: Elementary School
4201	3200060	00757	06: Rural - Fringe	ES: Elementary School
4101	3200060	00747	08: Suburb - Large	ES: Elementary School
4201	3200060	00753	08: Suburb - Large	ES: Elementary School
4201	3200060	00735	03: City - Midsize	PK: PreK

02	3200060	00744	04: City - Large	ES: Elementary School
4201	3200060	00732	04: City - Large	ES: Elementary School
4201	3200060	00733	08: Suburb - Large	ES: Elementary School
4201	3200060	00741	08: Suburb - Large	ES: Elementary School
4201	3200060	00736	08: Suburb - Large	ES: Elementary School
4202	3200060	00743	08: Suburb - Large	ES: Elementary School
4201	3200060	00737	08: Suburb - Large	ES: Elementary School
4203	3200060	00722	08: Suburb - Large	ES: Elementary School
4101	3200060	00689	08: Suburb - Large	ES: Elementary School
4201	3200060	00695	04: City - Large	ES: Elementary School
4101	3200060	00010	01: Rural - Distant	ES: Elementary School
4101	3200060	00080	01: Rural - Distant	ES: Elementary School
4101	3200060	00099	05: Rural - Remote	ES: Elementary School
4201	3200060	00343	08: Suburb - Large	ES: Elementary School
4101	3200060	00344	04: City - Large	ES: Elementary School
4201	3200060	00345	08: Suburb - Large	ES: Elementary School
4201	3200060	00346	03: City - Midsize	ES: Elementary School
4201	3200060	00354	04: City - Large	ES: Elementary School
4201	3200060	00355	04: City - Large	ES: Elementary School
4101	3200060	00356	04: City - Large	ES: Elementary School
4201	3200060	00357	08: Suburb - Large	ES: Elementary School
4101	3200060	00259	04: City - Large	ES: Elementary School
4201	3200060	00359	01: Rural - Distant	ES: Elementary School
4201	3200060	00371	08: Suburb - Large	ES: Elementary School
4201	3200060	00372	08: Suburb - Large	ES: Elementary School
4203	3200060	00373	04: City - Large	ES: Elementary School
4201	3200060	00260	04: City - Large	ES: Elementary School
4201	3200060	00375	04: City - Large	ES: Elementary School
4101	3200060	00376	04: City - Large	ES: Elementary School
4201	3200060	00377	08: Suburb - Large	ES: Elementary School
4201	3200060	00378	03: City - Midsize	ES: Elementary School
4203	3200060	00379	04: City - Large	ES: Elementary School
4201	3200060	00380	04: City - Large	ES: Elementary School
4201	3200060	00381	08: Suburb - Large	ES: Elementary School
4101	3200060	00382	04: City - Large	ES: Elementary School

4201	3200060	00383	04: City - Large	ES: Elementary School
4201	3200060	00401	08: Suburb - Large	ES: Elementary School
4201	3200060	00397	08: Suburb - Large	ES: Elementary School
4201	3200060	00396	03: City - Midsize	ES: Elementary School
4101	3200060	00395	08: Suburb - Large	ES: Elementary School
4201	3200060	00400	04: City - Large	ES: Elementary School
4202	3200060	00264	04: City - Large	ES: Elementary School
4201	3200060	00265	04: City - Large	ES: Elementary School
4203	3200060	00398	08: Suburb - Large	ES: Elementary School
4101	3200060	00399	02: Town - Fringe	ES: Elementary School
4201	3200060	00045	04: City - Large	ES: Elementary School
4203	3200060	00060	08: Suburb - Large	ES: Elementary School
4201	3200060	00076	04: City - Large	ES: Elementary School
4201	3200060	00077	08: Suburb - Large	ES: Elementary School
4201	3200060	00266	04: City - Large	ES: Elementary School
4203	3200060	00268	03: City - Midsize	ES: Elementary School
4201	3200060	00269	08: Suburb - Large	ES: Elementary School
4201	3200060	00270	08: Suburb - Large	ES: Elementary School
4201	3200060	00271	04: City - Large	ES: Elementary School
4201	3200060	00272	04: City - Large	ES: Elementary School
4201	3200060	00417	08: Suburb - Large	ES: Elementary School
4201	3200060	00434	04: City - Large	ES: Elementary School
4201	3200060	00435	08: Suburb - Large	ES: Elementary School
4201	3200060	00436	04: City - Large	ES: Elementary School
4101	3200060	00437	08: Suburb - Large	ES: Elementary School
4201	3200060	00438	08: Suburb - Large	ES: Elementary School
4201	3200060	00439	08: Suburb - Large	ES: Elementary School
4201	3200060	00440	04: City - Large	ES: Elementary School
4201	3200060	00441	04: City - Large	ES: Elementary School
4201	3200060	00442	08: Suburb - Large	ES: Elementary School
4201	3200060	00454	04: City - Large	ES: Elementary School
4201	3200060	00455	03: City - Midsize	ES: Elementary School
4201	3200060	00456	06: Rural - Fringe	ES: Elementary School
4101	3200060	00457	04: City - Large	ES: Elementary School
4203	3200060	00458	08: Suburb - Large	ES: Elementary School

4203	3200060	00459	04: City - Large	ES: Elementary School
4201	3200060	00469	04: City - Large	ES: Elementary School
4201	3200060	00470	08: Suburb - Large	ES: Elementary School
4201	3200060	00471	08: Suburb - Large	ES: Elementary School
4201	3200060	00472	04: City - Large	ES: Elementary School
4201	3200060	00473	04: City - Large	ES: Elementary School
4201	3200060	00485	08: Suburb - Large	ES: Elementary School
4201	3200060	00486	04: City - Large	ES: Elementary School
4101	3200060	00487	04: City - Large	ES: Elementary School
4201	3200060	00526	04: City - Large	ES: Elementary School
4201	3200060	00527	08: Suburb - Large	ES: Elementary School
4203	3200060	00528	04: City - Large	ES: Elementary School
4201	3200060	00529	08: Suburb - Large	ES: Elementary School
4201	3200060	00530	08: Suburb - Large	ES: Elementary School
4201	3200060	00531	04: City - Large	ES: Elementary School
4201	3200060	00532	08: Suburb - Large	ES: Elementary School
4201	3200060	00547	08: Suburb - Large	ES: Elementary School
4201	3200060	00548	08: Suburb - Large	ES: Elementary School
4201	3200060	00549	08: Suburb - Large	ES: Elementary School
4201	3200060	00550	03: City - Midsize	ES: Elementary School
4201	3200060	00551	08: Suburb - Large	ES: Elementary School
4201	3200060	00552	04: City - Large	ES: Elementary School
4201	3200060	00573	04: City - Large	ES: Elementary School
4201	3200060	00605	04: City - Large	ES: Elementary School
4201	3200060	00581	08: Suburb - Large	ES: Elementary School
4101	3200060	00580	03: City - Midsize	ES: Elementary School
4201	3200060	00623	04: City - Large	ES: Elementary School
4201	3200060	00574	08: Suburb - Large	ES: Elementary School
4203	3200060	00621	08: Suburb - Large	ES: Elementary School
4201	3200060	00652	08: Suburb - Large	ES: Elementary School
4201	3200060	00653	08: Suburb - Large	ES: Elementary School
4101	3200060	00654	08: Suburb - Large	ES: Elementary School
4201	3200060	00655	08: Suburb - Large	ES: Elementary School
4203	3200060	00656	08: Suburb - Large	ES: Elementary School
4101	3200060	00657	08: Suburb - Large	ES: Elementary School

4101	3200060	00658	08: Suburb - Large	ES: Elementary School
4201	3200060	00690	04: City - Large	ES: Elementary School
4201	3200060	00679	08: Suburb - Large	ES: Elementary School
4201	3200060	00716	08: Suburb - Large	ES: Elementary School
4201	3200060	00008	04: City - Large	ES: Elementary School
4201	3200060	00072	04: City - Large	ES: Elementary School
4201	3200060	00014	04: City - Large	ES: Elementary School
4203	3200060	00015	08: Suburb - Large	ES: Elementary School
4201	3200060	00023	04: City - Large	ES: Elementary School
4201	3200060	00016	08: Suburb - Large	ES: Elementary School
4203	3200060	00027	04: City - Large	ES: Elementary School
4203	3200060	00028	04: City - Large	ES: Elementary School
4201	3200060	00033	08: Suburb - Large	ES: Elementary School
4205	3200060	00039	04: City - Large	ES: Elementary School
4101	3200060	00063	04: City - Large	ES: Elementary School
4201	3200060	00050	04: City - Large	ES: Elementary School
4203	3200060	00052	08: Suburb - Large	ES: Elementary School
4205	3200060	00054	03: City - Midsize	ES: Elementary School
4201	3200060	00384	03: City - Midsize	OC: Other Combination
4201	3200060	00061	04: City - Large	ES: Elementary School
4201	3200060	00058	08: Suburb - Large	ES: Elementary School
4201	3200060	00055	04: City - Large	ES: Elementary School
4201	3200060	00064	04: City - Large	ES: Elementary School
4368	3200060	00066	08: Suburb - Large	ES: Elementary School
4201	3200060	00067	03: City - Midsize	ES: Elementary School
4201	3200060	00068	08: Suburb - Large	ES: Elementary School
4201	3200060	00069	08: Suburb - Large	ES: Elementary School
4201	3200060	00073	04: City - Large	ES: Elementary School
4201	3200060	00074	08: Suburb - Large	ES: Elementary School
4202	3200060	00075	04: City - Large	ES: Elementary School
5201	3200060	00797	04: City - Large	PK: PreK
4203	3200060	00079	08: Suburb - Large	ES: Elementary School
4201	3200060	00583	04: City - Large	ES: Elementary School
4201	3200060	00082	04: City - Large	ES: Elementary School
4201	3200060	00085	03: City - Midsize	ES: Elementary School

4201	3200060	00087	04: City - Large	ES: Elementary School
4101	3200060	00088	08: Suburb - Large	ES: Elementary School
4201	3200060	00090	04: City - Large	ES: Elementary School
4203	3200060	00091	04: City - Large	ES: Elementary School
4101	3200060	00092	08: Suburb - Large	ES: Elementary School
4201	3200060	00095	04: City - Large	ES: Elementary School
4201	3200060	00097	03: City - Midsize	ES: Elementary School
4203	3200060	00102	04: City - Large	ES: Elementary School
4201	3200060	00104	08: Suburb - Large	ES: Elementary School
4203	3200060	00105	04: City - Large	ES: Elementary School
4101	3200060	00106	04: City - Large	ES: Elementary School
4201	3200060	00109	04: City - Large	ES: Elementary School
4201	3200060	00112	04: City - Large	ES: Elementary School
4201	3200060	00046	04: City - Large	ES: Elementary School
4000	3200060	00116	08: Suburb - Large	ES: Elementary School
4201	3200060	00038	04: City - Large	ES: Elementary School
4101	3200060	00012	02: Town - Fringe	ES: Elementary School
4203	3200060	00019	04: City - Large	ES: Elementary School
4203	3200060	00577	05: Rural - Remote	ES: Elementary School
4203	3200060	00584	08: Suburb - Large	ES: Elementary School
4201	3200060	00093	04: City - Large	ES: Elementary School
4201	3200060	00110	07: Town - Distant	ES: Elementary School
4201	3200060	00115	08: Suburb - Large	ES: Elementary School
4201	3200060	00118	03: City - Midsize	ES: Elementary School
4201	3200060	00035	03: City - Midsize	ES: Elementary School
4201	3200060	00024	08: Suburb - Large	ES: Elementary School
4201	3200060	00081	08: Suburb - Large	ES: Elementary School
4201	3200060	00040	03: City - Midsize	ES: Elementary School
4201	3200060	00036	03: City - Midsize	ES: Elementary School
4201	3200060	00086	08: Suburb - Large	ES: Elementary School
4102	3200060	00044	04: City - Large	ES: Elementary School
4201	3200060	00009	03: City - Midsize	ES: Elementary School
4201	3200060	00041	08: Suburb - Large	ES: Elementary School
4201	3200060	00031	04: City - Large	ES: Elementary School
4201	3200060	00026	03: City - Midsize	ES: Elementary School

4201	3200060	00022	08: Suburb - Large	ES: Elementary School
4203	3200060	00113	08: Suburb - Large	ES: Elementary School
4201	3200060	00585	04: City - Large	ES: Elementary School
4201	3200060	00586	08: Suburb - Large	ES: Elementary School
4203	3200060	00587	04: City - Large	ES: Elementary School
4203	3200060	00588	08: Suburb - Large	ES: Elementary School
4202	3200060	00292	04: City - Large	ES: Elementary School
4201	3200060	00290	04: City - Large	ES: Elementary School
4101	3200060	00297	04: City - Large	ES: Elementary School
4201	3200060	00298	08: Suburb - Large	ES: Elementary School
4201	3200060	00302	06: Rural - Fringe	ES: Elementary School
4201	3200060	00506	08: Suburb - Large	ES: Elementary School
4201	3200060	00507	08: Suburb - Large	ES: Elementary School
4201	3200060	00508	04: City - Large	ES: Elementary School
4201	3200060	00509	08: Suburb - Large	ES: Elementary School
4101	3200060	00510	08: Suburb - Large	ES: Elementary School
4201	3200060	00511	04: City - Large	ES: Elementary School
4201	3200060	00512	04: City - Large	ES: Elementary School
4201	3200060	00513	04: City - Large	ES: Elementary School
4203	3200060	00589	03: City - Midsize	ES: Elementary School
4201	3200060	00303	04: City - Large	ES: Elementary School
4201	3200060	00612	01: Rural - Distant	ES: Elementary School
4000	3200060	00331	10: Town - Remote	ES: Elementary School
4101	3200060	00337	08: Suburb - Large	ES: Elementary School
4101	3200060	00338	08: Suburb - Large	ES: Elementary School
4201	3200060	00339	04: City - Large	ES: Elementary School
4201	3200060	00340	08: Suburb - Large	ES: Elementary School
4101	3200060	00341	04: City - Large	ES: Elementary School
4101	3200060	00342	04: City - Large	ES: Elementary School
4201	3200060	00489	04: City - Large	ES: Elementary School
4144	3200060	00029	08: Suburb - Large	MS: Middle School
4203	3200060	00034	04: City - Large	MS: Middle School
4201	3200060	00047	04: City - Large	MS: Middle School
4201	3200060	00056	03: City - Midsize	MS: Middle School
4201	3200060	00051	08: Suburb - Large	MS: Middle School

4200	3200060	00053	04: City - Large	MS: Middle School
4203	3200060	00057	08: Suburb - Large	MS: Middle School
4205	3200060	00059	04: City - Large	MS: Middle School
4203	3200060	00062	04: City - Large	MS: Middle School
4205	3200060	00094	04: City - Large	MS: Middle School
4203	3200060	00096	04: City - Large	MS: Middle School
4207	3200060	00117	03: City - Midsize	MS: Middle School
4201	3200060	00738	04: City - Large	MS: Middle School
4201	3200060	00017	03: City - Midsize	MS: Middle School
4501	3200060	00042	03: City - Midsize	MS: Middle School
4203	3200060	00289	08: Suburb - Large	MS: Middle School
4201	3200060	00291	02: Town - Fringe	MS: Middle School
4207	3200060	00301	04: City - Large	MS: Middle School
4201	3200060	00304	01: Rural - Distant	OC: Other Combination
4201	3200060	00408	06: Rural - Fringe	OC: Other Combination
4203	3200060	00404	06: Rural - Fringe	MS: Middle School
4201	3200060	00403	04: City - Large	MS: Middle School
4502	3200060	00402	04: City - Large	MS: Middle School
4201	3200060	00084	08: Suburb - Large	MS: Middle School
4201	3200060	00127	04: City - Large	MS: Middle School
4501	3200060	00273	04: City - Large	MS: Middle School
4502	3200060	00274	08: Suburb - Large	MS: Middle School
4201	3200060	00275	10: Town - Remote	MS: Middle School
02	3200060	00460	04: City - Large	OC: Other Combination
4201	3200060	00461	04: City - Large	MS: Middle School
4203	3200060	00462	08: Suburb - Large	MS: Middle School
4205	3200060	00474	04: City - Large	MS: Middle School
4201	3200060	00475	03: City - Midsize	MS: Middle School
4201	3200060	00476	08: Suburb - Large	MS: Middle School
4203	3200060	00699	05: Rural - Remote	MS: Middle School
4206	3200060	00490	08: Suburb - Large	MS: Middle School
4204	3200060	00514	04: City - Large	MS: Middle School
4203	3200060	00515	04: City - Large	MS: Middle School
4505	3200060	00534	04: City - Large	MS: Middle School
4201	3200060	00535	08: Suburb - Large	MS: Middle School

4056	3200060	00536	08: Suburb - Large	MS: Middle School
4101	3200060	00537	03: City - Midsize	MS: Middle School
4201	3200060	00538	08: Suburb - Large	MS: Middle School
4211	3200060	00553	08: Suburb - Large	MS: Middle School
4204	3200060	00554	08: Suburb - Large	MS: Middle School
4201	3200060	00590	04: City - Large	MS: Middle School
4205	3200060	00591	08: Suburb - Large	MS: Middle School
4500	3200060	00592	07: Town - Distant	MS: Middle School
4203	3200060	00570	08: Suburb - Large	MS: Middle School
4502	3200060	00578	04: City - Large	MS: Middle School
4207	3200060	00565	08: Suburb - Large	MS: Middle School
4201	3200060	00659	04: City - Large	MS: Middle School
4101	3200060	00660	08: Suburb - Large	MS: Middle School
4208	3200060	00663	08: Suburb - Large	MS: Middle School
4201	3200060	00672	08: Suburb - Large	MS: Middle School
4203	3200060	00700	08: Suburb - Large	MS: Middle School
4207	3200060	00739	04: City - Large	MS: Middle School
4203	3200060	00730	08: Suburb - Large	MS: Middle School
4203	3200060	00947	08: Suburb - Large	MS: Middle School
4201	3200060	00945	08: Suburb - Large	MS: Middle School
4205	3200060	00030	04: City - Large	HS: High School
4203	3200060	00065	08: Suburb - Large	HS: High School
4203	3200060	00089	08: Suburb - Large	HS: High School
4203	3200060	00107	08: Suburb - Large	HS: High School
4201	3200060	00114	04: City - Large	HS: High School
4211	3200060	00007	04: City - Large	HS: High School
5100	3200060	00103	04: City - Large	HS: High School
4203	3200060	00018	03: City - Midsize	HS: High School
4201	3200060	00032	08: Suburb - Large	HS: High School
4201	3200060	00011	04: City - Large	HS: High School
4201	3200060	00796	03: City - Midsize	HS: High School
4207	3200060	00406	04: City - Large	HS: High School
4210	3200060	00405	08: Suburb - Large	HS: High School
4201	3200060	00407	04: City - Large	HS: High School
4503	3200060	00276	08: Suburb - Large	HS: High School

4203	3200060	00277	04: City - Large	HS: High School
4201	3200060	00419	04: City - Large	HS: High School
4201	3200060	00420	03: City - Midsize	HS: High School
	3200060	00443	08: Suburb - Large	HS: High School
	3200060	00444	04: City - Large	HS: High School
4205	3200060	00445	08: Suburb - Large	HS: High School
4202	3200060	00446	04: City - Large	HS: High School
	3200060	00463	04: City - Large	HS: High School
4203	3200060	00595	04: City - Large	HS: High School
4203	3200060	00604	04: City - Large	HS: High School
4211	3200060	00567	08: Suburb - Large	HS: High School
4211	3200060	00571	03: City - Midsize	HS: High School
4205	3200060	00616	08: Suburb - Large	HS: High School
4501	3200060	00778	04: City - Large	HS: High School
4205	3200060	00780	08: Suburb - Large	HS: High School
4201	3200060	00777	08: Suburb - Large	HS: High School
4503	3200060	00812	06: Rural - Fringe	HS: High School
4201	3200060	00967	03: City - Midsize	ES: Elementary School
4500	3200060	00013	02: Town - Fringe	HS: High School
4201	3200060	00078	10: Town - Remote	HS: High School
4203	3200060	00111	07: Town - Distant	HS: High School
4203	3200060	00686	05: Rural - Remote	HS: High School
4205	3200060	00493	04: City - Large	HS: High School
4207	3200060	00494	04: City - Large	HS: High School
4201	3200060	00495	04: City - Large	HS: High School
4149	3200060	00539	08: Suburb - Large	HS: High School
4209	3200060	00540	04: City - Large	HS: High School
4207	3200060	00661	04: City - Large	HS: High School
4211	3200060	00714	08: Suburb - Large	HS: High School
4200	3200060	00755	04: City - Large	HS: High School
4210	3200060	00754	06: Rural - Fringe	HS: High School
4209	3200060	00748	06: Rural - Fringe	HS: High School
4215	3200060	00845	03: City - Midsize	OC: Other Combination
4215	3200060	00949	03: City - Midsize	ES: Elementary School
4201	3200060	00970	04: City - Large	HS: High School

4201	3200060	00977	08: Suburb - Large	HS: High School
	3200060	00950	08: Suburb - Large	HS: High School
	3200060	00294	04: City - Large	OC: Other Combination
4201	3200060	00986	08: Suburb - Large	PK: PreK
4201	3200060	00994	08: Suburb - Large	HS: High School
	3200060		04: City - Large	PK: PreK
	3200060		04: City - Large	PK: PreK
	3200060		04: City - Large	PK: PreK
	3200060		04: City - Large	PK: PreK
	3200060		04: City - Large	PK: PreK
4201	3200060	00774	03: City - Midsize	OC: Other Combination
4203	3200060	00108	04: City - Large	OC: Other Combination
	3200060	00020	04: City - Large	OC: Other Combination
	3200060	00101	01: Rural - Distant	OC: Other Combination
4101	3200060	00694	04: City - Large	OC: Other Combination
4101	3200060	00607	04: City - Large	ES: Elementary School
5151	3200060	00518	06: Rural - Fringe	OC: Other Combination
4101	3200060	00313	03: City - Midsize	HS: High School
5351	3200060	00328	04: City - Large	HS: High School
5100	3200060	00329	04: City - Large	HS: High School
4101	3200060	00572	04: City - Large	ES: Elementary School
4101	3200060	00683	04: City - Large	OC: Other Combination
4201	3200060	00499	04: City - Large	OC: Other Combination
4501	3200060	00597	04: City - Large	OC: Other Combination
4004	3200060	00598	04: City - Large	OC: Other Combination
4203	3200060	00619	04: City - Large	ES: Elementary School
	3200060	00582	04: City - Large	OC: Other Combination
	3200060	00807	04: City - Large	ES: Elementary School
	3200060	00790	01: Rural - Distant	AD: Adult HS
4203	3200060	00795	04: City - Large	AD: Adult HS
	3200060	00785	01: Rural - Distant	AD: Adult HS
n/a	3200060	00794	08: Suburb - Large	OC: Other Combination
4201	3200060	00767	08: Suburb - Large	HS: High School
	3200060	00847	01: Rural - Distant	HS: High School
4101	3200060	00878	04: City - Large	OC: Other Combination

4101	3200060	00987	02: Town - Fringe	OC: Other Combination
	3200060	00968	03: City - Midsize	OC: Other Combination
	3200060	00923	04: City - Large	OC: Other Combination
	3200090	00121	07: Town - Distant	ES: Elementary School
	3200090	00124	06: Rural - Fringe	ES: Elementary School
	3200090	00307	06: Rural - Fringe	ES: Elementary School
	3200090	00347	07: Town - Distant	ES: Elementary School
	3200090	00447	02: Town - Fringe	ES: Elementary School
	3200090	00448	07: Town - Distant	ES: Elementary School
	3200090	00119	07: Town - Distant	MS: Middle School
	3200090	00422	07: Town - Distant	MS: Middle School
	3200090	00120	07: Town - Distant	HS: High School
	3200090	00122	06: Rural - Fringe	OC: Other Combination
	3200090	00348	01: Rural - Distant	OC: Other Combination
	3200090	00832	06: Rural - Fringe	HS: High School
	3200090	00951	06: Rural - Fringe	MS: Middle School
1759	3200090	00764	06: Rural - Fringe	OC: Other Combination
	3200090	00861	06: Rural - Fringe	AD: Adult HS
1674	3200090	00981	07: Town - Distant	OC: Other Combination
	3200120	00131	05: Rural - Remote	OC: Other Combination
	3200120	00132	05: Rural - Remote	ES: Elementary School
	3200120	00133	05: Rural - Remote	OC: Other Combination
	3200120	00134	05: Rural - Remote	OC: Other Combination
	3200120	00139	05: Rural - Remote	OC: Other Combination
	3200120	00931	10: Town - Remote	ES: Elementary School
	3200120	00129	10: Town - Remote	ES: Elementary School
	3200120	00135	10: Town - Remote	ES: Elementary School
	3200120	00140	10: Town - Remote	ES: Elementary School
	3200120	00125	05: Rural - Remote	ES: Elementary School
	3200120	00727	05: Rural - Remote	ES: Elementary School
	3200120	00141	05: Rural - Remote	ES: Elementary School
	3200120	00308	10: Town - Remote	ES: Elementary School
	3200120	00349	10: Town - Remote	ES: Elementary School
	3200120	00350	06: Rural - Fringe	ES: Elementary School
	3200120	00385	06: Rural - Fringe	ES: Elementary School

	3200120	00750	10: Town - Remote	MS: Middle School
	3200120	00674	05: Rural - Remote	MS: Middle School
	3200120	00685	05: Rural - Remote	MS: Middle School
	3200120	00326	06: Rural - Fringe	MS: Middle School
	3200120	00464	06: Rural - Fringe	MS: Middle School
	3200120	00692	05: Rural - Remote	MS: Middle School
	3200120	00684	05: Rural - Remote	MS: Middle School
	3200120	00728	10: Town - Remote	MS: Middle School
	3200120	00568	05: Rural - Remote	HS: High School
	3200120	00622	05: Rural - Remote	HS: High School
	3200120	00130	10: Town - Remote	OC: Other Combination
	3200120	00610	05: Rural - Remote	HS: High School
	3200120	00579	05: Rural - Remote	HS: High School
	3200120	00330	06: Rural - Fringe	HS: High School
	3200120	00449	10: Town - Remote	HS: High School
933	3200120	00839	10: Town - Remote	OC: Other Combination
963	3200120	00854	10: Town - Remote	AD: Adult HS
	3200120	00836	10: Town - Remote	PK: PreK
	3200120	00829	10: Town - Remote	PK: PreK
	3200120	00969	05: Rural - Remote	HS: High School
	3200150	00143	05: Rural - Remote	OC: Other Combination
	3200150	00144	05: Rural - Remote	OC: Other Combination
	3200150	00943	05: Rural - Remote	HS: High School
104	3200180	00146	05: Rural - Remote	ES: Elementary School
1207	3200180	00147	05: Rural - Remote	ES: Elementary School
1207	3200180	00148	05: Rural - Remote	OC: Other Combination
	3200210	00150	05: Rural - Remote	OC: Other Combination
	3200210	00151	05: Rural - Remote	OC: Other Combination
	3200210	00155	05: Rural - Remote	OC: Other Combination
	3200210	00156	05: Rural - Remote	OC: Other Combination
	3200210		10: Town - Remote	ES: Elementary School
	3200210	00157	10: Town - Remote	ES: Elementary School
	3200210	00153	05: Rural - Remote	ES: Elementary School
	3200210	00325	10: Town - Remote	ES: Elementary School
	3200210	00159	10: Town - Remote	OC: Other Combination

	3200210	00708	05: Rural - Remote	MS: Middle School
	3200210	00149	10: Town - Remote	HS: High School
	3200210	00154	05: Rural - Remote	HS: High School
	3200210	00858	10: Town - Remote	AD: Adult HS
	3200210	00982	10: Town - Remote	OC: Other Combination
	3200240	00165	10: Town - Remote	ES: Elementary School
	3200240	00866	06: Rural - Fringe	MS: Middle School
	3200240	00163	10: Town - Remote	HS: High School
	3200240	00162	05: Rural - Remote	OC: Other Combination
	3200240	00864	10: Town - Remote	AD: Adult HS
	3200270	00170	05: Rural - Remote	ES: Elementary School
	3200270	00166	05: Rural - Remote	ES: Elementary School
	3200270	00172	05: Rural - Remote	ES: Elementary School
	3200270	00173	05: Rural - Remote	ES: Elementary School
	3200270	00410	05: Rural - Remote	MS: Middle School
	3200270	00423	05: Rural - Remote	MS: Middle School
	3200270	00168	05: Rural - Remote	HS: High School
	3200270	00171	05: Rural - Remote	HS: High School
	3200270	00169	05: Rural - Remote	OC: Other Combination
	3200270	00865	05: Rural - Remote	AD: Adult HS
	3200270	00850	05: Rural - Remote	AD: Adult HS
0104	3200300	00174	02: Town - Fringe	ES: Elementary School
0203	3200300	00179	07: Town - Distant	ES: Elementary School
0306	3200300	00175	07: Town - Distant	ES: Elementary School
0502	3200300	00299	01: Rural - Distant	ES: Elementary School
0603	3200300	00704	07: Town - Distant	ES: Elementary School
0805	3200300	00386	02: Town - Fringe	MS: Middle School
	3200300	00387	07: Town - Distant	ES: Elementary School
1003	3200300	00450	02: Town - Fringe	ES: Elementary School
1106	3200300	00746	06: Rural - Fringe	ES: Elementary School
0205	3200300	00312	07: Town - Distant	MS: Middle School
0304	3200300	00311	07: Town - Distant	ES: Elementary School
0402	3200300	00424	01: Rural - Distant	MS: Middle School
0506	3200300	00810	07: Town - Distant	MS: Middle School
0110	3200300	00176	07: Town - Distant	HS: High School

0204	3200300	00178	05: Rural - Remote	OC: Other Combination
0306	3200300	00180	07: Town - Distant	HS: High School
0409	3200300	00310	02: Town - Fringe	HS: High School
0506	3200300	00555	01: Rural - Distant	HS: High School
0506	3200300	00768	01: Rural - Distant	OC: Other Combination
0502	3200300	00860	07: Town - Distant	AD: Adult HS
0029	3200300	00958	07: Town - Distant	OC: Other Combination
	3200300	00988	07: Town - Distant	OC: Other Combination
1024	3200330	00811	10: Town - Remote	ES: Elementary School
1024	3200330	00184	05: Rural - Remote	ES: Elementary School
1024	3200330	00479	10: Town - Remote	MS: Middle School
1024	3200330	00183	10: Town - Remote	HS: High School
1024	3200330	00859	10: Town - Remote	AD: Adult HS
	3200360	00191	06: Rural - Fringe	ES: Elementary School
	3200360	00193	05: Rural - Remote	ES: Elementary School
	3200360	00189	05: Rural - Remote	ES: Elementary School
	3200360	00185	05: Rural - Remote	ES: Elementary School
	3200360	00351	10: Town - Remote	ES: Elementary School
	3200360	00186	05: Rural - Remote	ES: Elementary School
	3200360	00194	05: Rural - Remote	ES: Elementary School
	3200360	00425	10: Town - Remote	ES: Elementary School
	3200360	00543	06: Rural - Fringe	ES: Elementary School
	3200360	00752	06: Rural - Fringe	ES: Elementary School
	3200360	00412	06: Rural - Fringe	MS: Middle School
	3200360	00566	05: Rural - Remote	MS: Middle School
	3200360	00618	05: Rural - Remote	MS: Middle School
	3200360	00611	05: Rural - Remote	MS: Middle School
	3200360	00575	05: Rural - Remote	MS: Middle School
	3200360	00564	05: Rural - Remote	MS: Middle School
	3200360	00187	05: Rural - Remote	HS: High School
	3200360	00190	05: Rural - Remote	HS: High School
	3200360	00195	05: Rural - Remote	HS: High School
	3200360	00192	10: Town - Remote	HS: High School
	3200360	00363	05: Rural - Remote	HS: High School
	3200360	00557	10: Town - Remote	HS: High School

	3200360	00556	10: Town - Remote	MS: Middle School
	3200360	00852	10: Town - Remote	ES: Elementary School
	3200360	00862	10: Town - Remote	AD: Adult HS
	3200390	00288	09: City - Small	ES: Elementary School
	3200390	00792	09: City - Small	AD: Adult HS
	3200390	00286	09: City - Small	ES: Elementary School
	3200390	00285	09: City - Small	ES: Elementary School
	3200390	00282	09: City - Small	ES: Elementary School
	3200390	00364	09: City - Small	ES: Elementary School
	3200390	00160	09: City - Small	ES: Elementary School
	3200390	00569	09: City - Small	ES: Elementary School
	3200390	00281	09: City - Small	MS: Middle School
	3200390	00315	09: City - Small	MS: Middle School
	3200390	00280	09: City - Small	HS: High School
	3200420	00196	05: Rural - Remote	ES: Elementary School
	3200420	00197	05: Rural - Remote	ES: Elementary School
	3200420	00167	05: Rural - Remote	MS: Middle School
	3200420	00198	05: Rural - Remote	HS: High School
	3200420	00867	05: Rural - Remote	AD: Adult HS
	3200420	00762	05: Rural - Remote	
	3200450	00200	01: Rural - Distant	ES: Elementary School
	3200450	00413	06: Rural - Fringe	ES: Elementary School
	3200450	00365	01: Rural - Distant	MS: Middle School
	3200450	00199	01: Rural - Distant	HS: High School
	3200480	00203	04: City - Large	ES: Elementary School
	3200480	00209	04: City - Large	ES: Elementary School
	3200480	00212	04: City - Large	ES: Elementary School
	3200480	00218	04: City - Large	ES: Elementary School
	3200480	00219	04: City - Large	ES: Elementary School
	3200480	00223	04: City - Large	ES: Elementary School
	3200480	00226	04: City - Large	ES: Elementary School
	3200480	00230	04: City - Large	ES: Elementary School
	3200480	00232	04: City - Large	ES: Elementary School
	3200480	00558	04: City - Large	ES: Elementary School
	3200480	00321	04: City - Large	OC: Other Combination

	3200480	00559	04: City - Large	ES: Elementary School
	3200480	00236	04: City - Large	ES: Elementary School
	3200480	00240	04: City - Large	ES: Elementary School
	3200480	00242	04: City - Large	ES: Elementary School
	3200480	00243	04: City - Large	ES: Elementary School
	3200480	00245	04: City - Large	ES: Elementary School
	3200480	00248	04: City - Large	ES: Elementary School
	3200480	00251	04: City - Large	ES: Elementary School
	3200480	00201	08: Suburb - Large	ES: Elementary School
	3200480	00202	08: Suburb - Large	ES: Elementary School
	3200480	00214	08: Suburb - Large	ES: Elementary School
	3200480	00220	08: Suburb - Large	ES: Elementary School
	3200480	00227	08: Suburb - Large	ES: Elementary School
	3200480	00229	08: Suburb - Large	ES: Elementary School
	3200480	00231	08: Suburb - Large	ES: Elementary School
	3200480	00241	08: Suburb - Large	ES: Elementary School
	3200480	00205	08: Suburb - Large	ES: Elementary School
	3200480	00222	04: City - Large	ES: Elementary School
	3200480	00834	04: City - Large	ES: Elementary School
	3200480	00228	08: Suburb - Large	ES: Elementary School
	3200480	00237	08: Suburb - Large	ES: Elementary School
	3200480	00249	08: Suburb - Large	ES: Elementary School
	3200480	00250	07: Town - Distant	ES: Elementary School
	3200480	00234	07: Town - Distant	ES: Elementary School
	3200480	00320	08: Suburb - Large	ES: Elementary School
	3200480	00319	08: Suburb - Large	ES: Elementary School
	3200480	00324	08: Suburb - Large	ES: Elementary School
	3200480	00723	06: Rural - Fringe	ES: Elementary School
	3200480	00706	08: Suburb - Large	ES: Elementary School
	3200480	00936	04: City - Large	ES: Elementary School
	3200480	00942	08: Suburb - Large	ES: Elementary School
	3200480	00960	08: Suburb - Large	ES: Elementary School
	3200480	00978	04: City - Large	ES: Elementary School
	3200480	00224	07: Town - Distant	ES: Elementary School
	3200480	00322	08: Suburb - Large	ES: Elementary School

	3200480	00317	08: Suburb - Large	ES: Elementary School
	3200480	00316	04: City - Large	ES: Elementary School
	3200480	00336	08: Suburb - Large	ES: Elementary School
	3200480	00388	04: City - Large	ES: Elementary School
	3200480	00389	04: City - Large	ES: Elementary School
	3200480	00366	08: Suburb - Large	ES: Elementary School
	3200480	00367	04: City - Large	ES: Elementary School
	3200480	00368	04: City - Large	ES: Elementary School
	3200480	00390	08: Suburb - Large	ES: Elementary School
	3200480	00414	08: Suburb - Large	ES: Elementary School
	3200480	00221	08: Suburb - Large	ES: Elementary School
	3200480	00426	04: City - Large	ES: Elementary School
	3200480	00427	08: Suburb - Large	ES: Elementary School
	3200480	00428	04: City - Large	ES: Elementary School
	3200480	00432	08: Suburb - Large	ES: Elementary School
	3200480	00452	04: City - Large	ES: Elementary School
	3200480	00466	04: City - Large	ES: Elementary School
	3200480	00467	08: Suburb - Large	ES: Elementary School
	3200480	00481	08: Suburb - Large	ES: Elementary School
	3200480	00523	08: Suburb - Large	ES: Elementary School
	3200480	00544	04: City - Large	ES: Elementary School
	3200480	00961	04: City - Large	ES: Elementary School
	3200480	00979	04: City - Large	ES: Elementary School
	3200480	00560	04: City - Large	ES: Elementary School
	3200480	00561	04: City - Large	OC: Other Combination
	3200480	00204	04: City - Large	MS: Middle School
	3200480	00206	04: City - Large	MS: Middle School
	3200480	00207	04: City - Large	MS: Middle School
	3200480	00215	04: City - Large	MS: Middle School
	3200480	00216	08: Suburb - Large	MS: Middle School
	3200480	00247	08: Suburb - Large	MS: Middle School
	3200480	00235	04: City - Large	MS: Middle School
	3200480	00318	07: Town - Distant	MS: Middle School
	3200480	00391	04: City - Large	MS: Middle School
	3200480	00433	08: Suburb - Large	MS: Middle School

	3200480	00525	04: City - Large	HS: High School
	3200480	00678	04: City - Large	MS: Middle School
	3200480	00624	08: Suburb - Large	MS: Middle School
	3200480	00673	08: Suburb - Large	OC: Other Combination
	3200480	00682	04: City - Large	ES: Elementary School
	3200480	00913	08: Suburb - Large	MS: Middle School
	3200480	00880	04: City - Large	OC: Other Combination
	3200480	00932	06: Rural - Fringe	MS: Middle School
	3200480	00939	08: Suburb - Large	MS: Middle School
	3200480	00208	04: City - Large	HS: High School
	3200480	00239	04: City - Large	HS: High School
	3200480	00246	08: Suburb - Large	HS: High School
	3200480	00238	04: City - Large	HS: High School
	3200480	00210	08: Suburb - Large	HS: High School
	3200480	00822	04: City - Large	OC: Other Combination
	3200480	00323	04: City - Large	HS: High School
	3200480	00257	08: Suburb - Large	HS: High School
	3200480	00869	04: City - Large	HS: High School
	3200480	00995	04: City - Large	HS: High School
	3200480	00217	05: Rural - Remote	OC: Other Combination
	3200480	00225	07: Town - Distant	HS: High School
	3200480	00468	04: City - Large	HS: High School
	3200480	00503	04: City - Large	OC: Other Combination
	3200480	00545	06: Rural - Fringe	HS: High School
	3200480	00546	08: Suburb - Large	HS: High School
	3200480	00562	04: City - Large	HS: High School
	3200480	00602	04: City - Large	HS: High School
	3200480	00603	04: City - Large	HS: High School
	3200480	00664	04: City - Large	HS: High School
	3200480	00989	04: City - Large	PK: PreK
	3200480	00996	08: Suburb - Large	PK: PreK
	3200480	00233	08: Suburb - Large	OC: Other Combination
	3200480	00766	04: City - Large	OC: Other Combination
	3200480	00863	04: City - Large	AD: Adult HS
	3200480	00765	04: City - Large	HS: High School

	3200480	00844	04: City - Large	OC: Other Combination
	3200480	00985	04: City - Large	OC: Other Combination
	3200510	00720	05: Rural - Remote	ES: Elementary School
	3200510	00254	05: Rural - Remote	ES: Elementary School
2102	3200510	00255	10: Town - Remote	ES: Elementary School
	3200510	00263	10: Town - Remote	ES: Elementary School
5103	3200510	00776	10: Town - Remote	PK: PreK
3103	3200510	00256	10: Town - Remote	MS: Middle School
5102	3200510	00267	10: Town - Remote	HS: High School
2385	3200510	00606	05: Rural - Remote	OC: Other Combination
	3200510	00483	10: Town - Remote	HS: High School
	3200510	00857	10: Town - Remote	AD: Adult HS
	3200510	00984	10: Town - Remote	OC: Other Combination
	3200510		10: Town - Remote	OC: Other Combination
	3200001	00842	08: Suburb - Large	OC: Other Combination
	3200001	00895	08: Suburb - Large	OC: Other Combination
	3200001	00912	04: City - Large	OC: Other Combination
	3200001	00934	08: Suburb - Large	OC: Other Combination
	3200001	00881	03: City - Midsize	ES: Elementary School
	3200001	00896	04: City - Large	OC: Other Combination
			03: City - Midsize	PK: PreK
			03: City - Midsize	PK: PreK
			03: City - Midsize	PK: PreK
			03: City - Midsize	PK: PreK
			03: City - Midsize	PK: PreK
			03: City - Midsize	PK: PreK
			03: City - Midsize	PK: PreK
			03: City - Midsize	PK: PreK
			03: City - Midsize	PK: PreK
			03: City - Midsize	PK: PreK
			03: City - Midsize	PK: PreK
			03: City - Midsize	PK: PreK
			03: City - Midsize	PK: PreK
			03: City - Midsize	PK: PreK
			03: City - Midsize	PK: PreK
	3200001	01002	04: City - Large	OC: Other Combination
	3200001	00870	04: City - Large	OC: Other Combination

	3200001	00856	04: City - Large	OC: Other Combination
	3200001	01003	08: Suburb - Large	ES: Elementary School
	3200001	01004	08: Suburb - Large	ES: Elementary School
	3200001	00851	04: City - Large	OC: Other Combination
	3200001	00902	04: City - Large	OC: Other Combination
	3200001	00955	04: City - Large	OC: Other Combination
5076	3200001	00848	08: Suburb - Large	OC: Other Combination
5076	3200001	00956	08: Suburb - Large	ES: Elementary School
	3200001	00843	04: City - Large	OC: Other Combination
	3200001	00886	04: City - Large	OC: Other Combination
	3200001	00833	10: Town - Remote	OC: Other Combination
	3200001	00888	06: Rural - Fringe	OC: Other Combination
	3200001	00893	04: City - Large	OC: Other Combination
	3200001	00830	06: Rural - Fringe	OC: Other Combination
4227	3200001	00906	08: Suburb - Large	OC: Other Combination
2008	3200001	00892	08: Suburb - Large	OC: Other Combination
	3200001	00826	04: City - Large	OC: Other Combination
	3200001	00897	04: City - Large	ES: Elementary School
	3200001	00825	04: City - Large	OC: Other Combination
	3200001	00909	06: Rural - Fringe	OC: Other Combination
	3200001	00899	04: City - Large	OC: Other Combination
9700	3200001	00941	06: Rural - Fringe	OC: Other Combination
	3200001	00976	04: City - Large	OC: Other Combination
	3200001	00990	04: City - Large	ES: Elementary School
	3200001	00904	08: Suburb - Large	OC: Other Combination
	3200001	00898	08: Suburb - Large	OC: Other Combination
	3200001	00901	04: City - Large	OC: Other Combination
	3200001	00820	04: City - Large	OC: Other Combination
	3200001	00910	04: City - Large	OC: Other Combination
	3200001	00921	08: Suburb - Large	OC: Other Combination
	3200001	00911	06: Rural - Fringe	OC: Other Combination
	3200001	01005	03: City - Midsize	OC: Other Combination
	3200001	00885	03: City - Midsize	OC: Other Combination
	3200001	00818	04: City - Large	OC: Other Combination
	3200001	00997	08: Suburb - Large	ES: Elementary School

100	3200001	00740	04: City - Large	ES: Elementary School
	3200001	00817	10: Town - Remote	OC: Other Combination
	3200001	00891	06: Rural - Fringe	OC: Other Combination
4101	3200001	00745	04: City - Large	OC: Other Combination
	3200001	00784	10: Town - Remote	OC: Other Combination
	3200001	00717	04: City - Large	ES: Elementary School
	3200001	00749	04: City - Large	OC: Other Combination
1112	3200001	00759	04: City - Large	OC: Other Combination
	3200001	00821	04: City - Large	OC: Other Combination
	3200001	01006	04: City - Large	OC: Other Combination
	3200001	00800	08: Suburb - Large	HS: High School
8033	3200001	01007	04: City - Large	OC: Other Combination
	3200001	00781	04: City - Large	OC: Other Combination
	3200023	00808	02: Town - Fringe	HS: High School
	3200001	00900	04: City - Large	HS: High School
1101	3200001	00903	04: City - Large	HS: High School
	3200001	00608	04: City - Large	HS: High School
	3200001	00928	08: Suburb - Large	HS: High School
	3200001	00937	08: Suburb - Large	HS: High School
	3200001	00944	04: City - Large	HS: High School
	3200001	00948	04: City - Large	HS: High School
	3200001	00965	08: Suburb - Large	HS: High School
	3200021	00680	04: City - Large	OC: Other Combination
	3200001	00731	04: City - Large	HS: High School
	3200001	00734	03: City - Midsize	OC: Other Combination
	3200001	00908	04: City - Large	OC: Other Combination
	3200001	00907	08: Suburb - Large	OC: Other Combination
106	3200001	00742	04: City - Large	OC: Other Combination
107	3200001	00890	03: City - Midsize	ES: Elementary School
203	3200001	00894	04: City - Large	OC: Other Combination
302	3200001	00922	04: City - Large	OC: Other Combination
109	3200001	00966	08: Suburb - Large	OC: Other Combination
	3200001	00751	08: Suburb - Large	HS: High School
	3200001	00998	03: City - Midsize	MS: Middle School
1132		00993	08: Suburb - Large	HS: High School

	3200001	00999	04: City - Large	HS: High School
	3200001	01000	08: Suburb - Large	ES: Elementary School
	3200001	01008	10: Town - Remote	ES: Elementary School
	3200001	00917	03: City - Midsize	OC: Other Combination
1101	3200001	00924	04: City - Large	OC: Other Combination
	3200001	00938	04: City - Large	OC: Other Combination
	3200001	00953	08: Suburb - Large	OC: Other Combination
	3200001	00952	04: City - Large	OC: Other Combination
	3200001	00962	08: Suburb - Large	OC: Other Combination
	3200001	00972	03: City - Midsize	OC: Other Combination
	3200001	00974	04: City - Large	ES: Elementary School
			08: Suburb - Large	OC: Other Combination
	3200511	01010	04: City - Large	ES: Elementary School

[illegible]

[illegible]

[illegible]

Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
No	No		No	No
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
No	No		No	No
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
No	No		No	No
No	No		No	No
No	No		No	No
No	No		No	No
No	No		No	No
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
No	No		No	No
No	No		No	No
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
No	No		No	No
No	No		No	No
Yes	Yes	5: CEP	Yes	Yes
No	No		No	No
No	No		No	No
No	No		No	No
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
No	No		No	No
No	No		No	No
No	No		No	No
No	No		No	No
No	No		No	No
No	No		No	No
Yes	Yes	5: CEP	Yes	Yes
No	No		No	No
Yes	Yes	5: CEP	Yes	Yes

Yes	Yes	5: CEP	Yes	Yes
No	No		No	No
No	No		No	No
Yes	Yes		No	No
Yes	Yes		No	No
Yes	Yes		No	No
Yes	Yes		No	No
Yes	Yes		No	No
Yes	Yes		No	No
Yes	Yes		No	No
Yes	Yes		No	No
Yes	Yes		No	No
No	No		No	No
Yes	Yes	5: CEP	Yes	Yes
No	No		No	No
No	No		No	No
No	No		No	No
No	No		No	No
No	No		No	No
Yes	Yes		No	No
No	No		No	No
No	No		No	No
Yes	Yes		No	No
Yes	Yes		No	No
No	Yes		No	No
Yes	Yes		No	No
Yes	Yes		No	No
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes		No	No
Yes	Yes		No	No
Yes	Yes		No	No
Yes	Yes		No	No
Yes	Yes		No	No

Yes	Yes		No	No
Yes	Yes		No	No
Yes	Yes		No	No
No	Yes		No	No
No	Yes		No	No
Yes	Yes		No	No
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes		No	No
Yes	Yes		No	No
Yes	Yes		No	No
No	Yes		No	No
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes		No	No
No	Yes		No	No
Yes	Yes		No	No
No	No		No	No
No	No		No	No
No	No		No	No
No	No		No	No
No	No		No	No
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
No	No		No	No
No	No		No	No
No	No		No	No
No	No		No	No
No	No		No	No
No	No		No	No
No	No		No	No
No	No		No	No
Yes	Yes		No	No
Yes	Yes		No	No
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes		No	No
Yes	Yes		No	No

[illegible]

[illegible]

Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
No	No		No	No
Yes	Yes		No	No
No	No		No	No
Yes	Yes		No	No
No	No		No	No
Yes	Yes		No	No
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
No	No		No	No
Yes	Yes		No	No
Yes	Yes		No	No
Yes	Yes		No	No
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
No	No		No	No
No	No		No	No
No	No		No	No
Yes	Yes	5: CEP	Yes	Yes
No	No		No	No
No	No		No	No
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
No	Yes		No	No
Yes	Yes		No	No

Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
No	Yes		No	No
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
No	Yes		No	No
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes		No	No
Yes	Yes	5: CEP	Yes	Yes
No	Yes		No	No
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes		No	No
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes		No	No
Yes	Yes		No	No
Yes	Yes		No	No
Yes	Yes		No	No
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes

No	Yes		No	No
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
No	Yes		No	No
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
No	Yes		No	No
No	Yes		No	No
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes		No	No
Yes	Yes	5: CEP	Yes	Yes
No	Yes		No	No
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes		No	No
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
No	Yes		No	No
Yes	Yes	5: CEP	Yes	Yes
No	No		No	No
Yes	Yes	5: CEP	Yes	Yes
No	No		No	No
No	No		No	No
Yes	Yes	5: CEP	Yes	Yes
No	Yes		No	No
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes		No	No
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes		No	No
Yes	Yes		No	No
Yes	Yes	5: CEP	Yes	Yes

No	No		No	No
Yes	Yes		No	No
No	No		No	No
Yes	Yes	5: CEP	Yes	Yes
No	No		No	No
Yes	Yes		No	No
No	No		No	No
Yes	Yes	5: CEP	Yes	Yes
No	Yes		No	No
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes		No	No
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes		No	No
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes		No	No
Yes	Yes		No	No
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes		No	No
No	No		No	No
Yes	Yes		No	No
No	No		No	No
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes		No	No
Yes	Yes	5: CEP	Yes	Yes
No	No		No	No
Yes	Yes		No	No
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes		No	No
No	No		No	No
No	No		No	No
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
No	No		No	No
No	No		No	No

No	No		No	No
No	No		No	No
Yes	Yes	5: CEP	Yes	Yes
No	No		No	No
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
No	No		No	No
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
No	No		No	No
No	No		No	No
No	No		No	No
No	Yes		No	No
Yes	Yes		No	No
Yes	Yes		No	No
Yes	Yes		No	No
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
No	No		No	No
No	No		No	No
No	No		No	No
No	No		No	No
No	No		No	No
No	No		No	No
No	No		No	No
No	No		No	No
No	No		No	No
No	No		No	No
No	No		No	No
No	No		No	No
No	No		No	No
No	No		No	No
No	No		No	No
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes

Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
No	No		No	No
No	No		No	No
No	No		No	No
No	Yes		No	No
No	No		No	No
No	Yes		No	No
Yes	Yes		No	No
Yes	Yes		No	No
No	Yes		No	No
No	Yes		No	No
No	No		No	No
No	Yes		No	No
No	Yes		No	No
No	Yes		No	No
No	Yes		No	No
No	Yes		No	No
No	Yes		No	No
Yes	Yes		No	No
No	No		No	No
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes		No	No
Yes	Yes		No	No
No	Yes		No	No
No	Yes		No	No
Yes	Yes		No	No
No	Yes		No	No
No	Yes		No	No
No	No		No	No
Yes	Yes	5: CEP	Yes	Yes
No	No		No	No
Yes	Yes	5: CEP	Yes	Yes

Yes	Yes	5: CEP	Yes	Yes
No	No		No	No
No	Yes		No	No
Yes	Yes	5: CEP	Yes	Yes
No	Yes		No	No
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes		No	No
Yes	Yes	5: CEP	Yes	Yes
No	No		No	No
No	No		No	No
No	No		No	No
No	No		No	No
No	No		No	No
No	No		No	No
No	No		No	No
No	No		No	No
No	No		No	No
No	No		No	No
No	No		No	No
No	No		No	No
No	No		No	No
No	No		No	No
No	No		No	No
No	No		No	No
No	No		No	No
No	Yes		No	No
Yes	Yes		No	No
No	Yes		No	No
No	Yes		No	No
Yes	Yes		No	No
Yes	Yes		No	No
Yes	Yes		No	No
No	No		No	No
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes

No	No		No	No
Yes	Yes	5: CEP	Yes	Yes
No	No		No	No
Yes	Yes	5: CEP	Yes	Yes
No	No		No	No
No	Yes		No	No
Yes	Yes		No	No
Yes	Yes		No	No
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
Yes	Yes	5: CEP	Yes	Yes
No	No		No	No

Provision Base Year	Provision End Year	CEDS - NSLP Status	Eden
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPNO	Yes
2026	2030	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
0	0	NSLPNO	Yes

2026	2030	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2026	2029	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes

2025	2029	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2026	2029	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes

2026	2030	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes

2026	2030	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
0	0	NSLPNO	Yes
2024	2028	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes

2025	2029	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes

2026	2030	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes

2024	2028	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2023	2029	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes

2026	2030	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
0	0	NSLPNO	Yes
2025	2029	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2024	2027	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes

2025	2029	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
2024	2028	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
0	0	NSLPNO	Yes
2025	2029	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
2024	2028	NSLPCEO	Yes

2023	2027	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
0	0	NSLPNO	Yes
2025	2029	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
2026	2030	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
2025	2029	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
2026	2030	NSLPCEO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
2026	2030	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
2026	2030	NSLPCEO	Yes
0	0	NSLPNO	Yes
2025	2029	NSLPCEO	Yes

2026	2030	NSLPCEO	Yes
0	0	NSLPNO	No
0	0	NSLPNO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPNO	Yes
2023	2027	NSLPCEO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	No
0	0	NSLPNO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
2023	2027	NSLPCEO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes

0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
2023	2027	NSLPCEO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
2023	2027	NSLPCEO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
2024	2028	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
2026	2030	NSLPCEO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes

[illegible]

[illegible]

2025	2029	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
0	0	NSLPNO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPNO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPNO	Yes
0	0	NSLPWOPRO	Yes
2024	2028	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
0	0	NSLPNO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
2026	2030	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
2026	2030	NSLPCEO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
2024	2028	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes

2024	2028	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
0	0	NSLPWOPRO	Yes
2024	2028	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
0	0	NSLPWOPRO	Yes
2024	2028	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
0	0	NSLPWOPRO	Yes
2024	2028	NSLPCEO	Yes
0	0	NSLPWOPRO	Yes
2024	2028	NSLPCEO	Yes
0	0	NSLPWOPRO	Yes
2024	2028	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
0	0	NSLPWOPRO	Yes
2024	2028	NSLPCEO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
2024	2028	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes

0	0	NSLPWOPRO	Yes
2024	2028	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
0	0	NSLPWOPRO	Yes
2024	2028	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
2024	2028	NSLPCEO	Yes
0	0	NSLPWOPRO	Yes
2024	2028	NSLPCEO	Yes
0	0	NSLPWOPRO	Yes
2024	2028	NSLPCEO	Yes
0	0	NSLPWOPRO	Yes
2024	2028	NSLPCEO	Yes
0	0	NSLPWOPRO	Yes
2024	2028	NSLPCEO	Yes
0	0	NSLPWOPRO	Yes
2024	2028	NSLPCEO	Yes
0	0	NSLPNO	Yes
2024	2028	NSLPCEO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
2024	2028	NSLPCEO	Yes
0	0	NSLPWOPRO	Yes
2026	2030	NSLPCEO	Yes
0	0	NSLPWOPRO	Yes
2024	2028	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
2024	2028	NSLPCEO	Yes

0	0	NSLPNO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPNO	Yes
2024	2028	NSLPCEO	Yes
0	0	NSLPNO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPNO	Yes
2024	2028	NSLPCEO	Yes
0	0	NSLPWOPRO	Yes
2024	2028	NSLPCEO	Yes
0	0	NSLPWOPRO	Yes
2024	2028	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
0	0	NSLPWOPRO	Yes
2024	2028	NSLPCEO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
2024	2028	NSLPCEO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPNO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPNO	Yes
2026	2030	NSLPCEO	Yes
0	0	NSLPWOPRO	Yes
2024	2028	NSLPCEO	Yes
0	0	NSLPNO	Yes
0	0	NSLPWOPRO	Yes
2024	2028	NSLPCEO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPNO	No
0	0	NSLPNO	Yes
2024	2028	NSLPCEO	Yes
2024	2028	NSLPCEO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes

0	0	NSLPNO	Yes
0	0	NSLPNO	No
2025	2029	NSLPCEO	Yes
0	0	NSLPNO	Yes
2025	2029	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
0	0	NSLPNO	Yes
2025	2029	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	No
0	0	NSLPNO	No
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
2026	2030	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
0	0	NSLPNO	No
0	0	NSLPNO	No
0	0	NSLPNO	No
0	0	NSLPNO	No
0	0	NSLPNO	No
0	0	NSLPNO	No
0	0	NSLPNO	No
0	0	NSLPNO	No
0	0	NSLPNO	No
0	0	NSLPNO	No
0	0	NSLPNO	No
0	0	NSLPNO	No
0	0	NSLPNO	No
2026	2030	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes

2023	2027	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2024	2027	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPNO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPNO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPNO	Yes
2025	2029	NSLPCEO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPNO	Yes
2026	2030	NSLPCEO	Yes
0	0	NSLPNO	Yes
2026	2030	NSLPCEO	Yes

2025	2029	NSLPCEO	Yes
0	0	NSLPNO	Yes
0	0	NSLPWOPRO	Yes
2026	2030	NSLPCEO	Yes
0	0	NSLPWOPRO	Yes
2025	2029	NSLPCEO	Yes
2025	2029	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes
0	0	NSLPWOPRO	Yes
2025	2029	NSLPCEO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
0	0	NSLPNO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPNO	Yes
2026	2030	NSLPCEO	Yes
2026	2030	NSLPCEO	Yes

0	0	NSLPNO	Yes
2025	2029	NSLPCEO	Yes
0	0	NSLPNO	Yes
2024	2028	NSLPCEO	Yes
0	0	NSLPNO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
0	0	NSLPWOPRO	Yes
2025	2029	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2023	2027	NSLPCEO	Yes
2026	2030	NSLPCEO	No
0	0	NSLPNO	Yes

Title 1	Title 1 Served	Magnet Status	SharedTimeStatus	APF
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		Yes	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGYES: Magnet Yes	No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No

SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No

SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No	MAGYES: Magnet Yes	No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No

SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No	MAGYES: Magnet Yes	No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		Yes	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No

SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No	MAGYES: Magnet Yes	No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGYES: Magnet Yes	No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	Yes
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGYES: Magnet Yes	No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No

[illegible]

SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGYES: Magnet Yes	No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No	MAGYES: Magnet Yes	No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No	MAGYES: Magnet Yes	No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGYES: Magnet Yes	No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No

SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGYES: Magnet Yes	No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGYES: Magnet Yes	Yes	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGYES: Magnet Yes	Yes	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGYES: Magnet Yes	No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGYES: Magnet Yes	No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No	MAGYES: Magnet Yes	No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGYES: Magnet Yes	No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No	MAGYES: Magnet Yes	No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No	MAGYES: Magnet Yes	Yes	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No	MAGYES: Magnet Yes	No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		Yes	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No	MAGYES: Magnet Yes	Yes	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No		Yes	No
NOTTITLE1ELIG: Not a Title I School	No		Yes	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		Yes	No

SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		Yes	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		Yes	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		Yes	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		Yes	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGYES: Magnet Yes	No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No	MAGYES: Magnet Yes	No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGYES: Magnet Yes	Yes	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGYES: Magnet Yes	No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGYES: Magnet Yes	No	No
SWELIGSWPROG: Schoolwide Program	Yes		Yes	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGYES: Magnet Yes	No	No
NOTTITLE1ELIG: Not a Title I School	No		Yes	Yes
SWELIGSWPROG: Schoolwide Program	Yes		Yes	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGYES: Magnet Yes	Yes	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No	MAGYES: Magnet Yes	No	No
SWELIGSWPROG: Schoolwide Program	Yes		Yes	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		Yes	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		Yes	No

NOTTITLE1ELIG: Not a Title I School	No	MAGYES: Magnet Yes	No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No	MAGYES: Magnet Yes	No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		Yes	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		Yes	No
NOTTITLE1ELIG: Not a Title I School	No		Yes	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		Yes	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		Yes	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGYES: Magnet Yes	No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGYES: Magnet Yes	No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No	MAGYES: Magnet Yes	Yes	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No	MAGYES: Magnet Yes	No	No
NOTTITLE1ELIG: Not a Title I School	No	MAGYES: Magnet Yes	No	No
SWELIGSWPROG: Schoolwide Program	Yes		Yes	No
NOTTITLE1ELIG: Not a Title I School	No	MAGYES: Magnet Yes	No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		Yes	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		Yes	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		Yes	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGYES: Magnet Yes	Yes	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		Yes	No
NOTTITLE1ELIG: Not a Title I School	No		Yes	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		Yes	No
SWELIGSWPROG: Schoolwide Program	Yes		Yes	No
NOTTITLE1ELIG: Not a Title I School	No	MAGYES: Magnet Yes	No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		Yes	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No	MAGYES: Magnet Yes	No	No
NOTTITLE1ELIG: Not a Title I School	No		Yes	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No	MAGNO: Magnet No	No	No

SWELIGNOPROG: Schoolwide Eligible - No Program	No	MAGYES: Magnet Yes	No	No
SWELIGSWPROG: Schoolwide Program	Yes		Yes	No
NOTTITLE1ELIG: Not a Title I School	No		Yes	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	Yes
SWELIGSWPROG: Schoolwide Program	Yes		No	Yes
NOTTITLE1ELIG: Not a Title I School	No		Yes	Yes
NOTTITLE1ELIG: Not a Title I School	No		Yes	Yes
SWELIGSWPROG: Schoolwide Program	Yes		No	Yes
SWELIGSWPROG: Schoolwide Program	Yes		No	Yes
NOTTITLE1ELIG: Not a Title I School	No		No	Yes
NOTTITLE1ELIG: Not a Title I School	No		Yes	Yes
SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No		Yes	Yes
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	Yes
SWELIGSWPROG: Schoolwide Program	Yes		No	Yes
SWELIGSWPROG: Schoolwide Program	Yes		Yes	Yes
SWELIGSWPROG: Schoolwide Program	Yes		No	Yes
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		Yes	Yes
NOTTITLE1ELIG: Not a Title I School	No		Yes	No
NOTTITLE1ELIG: Not a Title I School	No		Yes	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		Yes	Yes
NOTTITLE1ELIG: Not a Title I School	No		Yes	No
SWELIGSWPROG: Schoolwide Program	Yes		No	Yes

SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		Yes	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	Yes
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No

SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No

[illegible]

SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	Yes
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		Yes	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGNO: Magnet No	No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGNO: Magnet No	No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGNO: Magnet No	No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGNO: Magnet No	No	No
NOTTITLE1ELIG: Not a Title I School	No	MAGNO: Magnet No	No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	Yes

SWELIGSWPROG: Schoolwide Program	Yes		No	Yes
NOTTITLE1ELIG: Not a Title I School	No		No	Yes
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGNO: Magnet No	No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGNO: Magnet No	No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGNO: Magnet No	No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGNO: Magnet No	No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No	MAGNO: Magnet No	No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No	MAGNO: Magnet No	No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGNO: Magnet No	No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No	MAGNO: Magnet No	No	No
NOTTITLE1ELIG: Not a Title I School	No	MAGNO: Magnet No	No	No
NOTTITLE1ELIG: Not a Title I School	No	MAGNO: Magnet No	No	No

SWELIGNOPROG: Schoolwide Eligible - No Program	No	MAGNO: Magnet No	No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGNO: Magnet No	No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGNO: Magnet No	No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGNO: Magnet No	No	No
NOTTITLE1ELIG: Not a Title I School	No	MAGNO: Magnet No	No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGNO: Magnet No	No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGNO: Magnet No	No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGNO: Magnet No	No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGNO: Magnet No	No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGNO: Magnet No	No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGNO: Magnet No	No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGNO: Magnet No	No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGNO: Magnet No	No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No	MAGNO: Magnet No	No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGNO: Magnet No	No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGNO: Magnet No	No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No	MAGNO: Magnet No	No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No	MAGNO: Magnet No	No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGNO: Magnet No	No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGNO: Magnet No	No	No
NOTTITLE1ELIG: Not a Title I School	No	MAGNO: Magnet No	No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGNO: Magnet No	No	No
NOTTITLE1ELIG: Not a Title I School	No	MAGNO: Magnet No	No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGNO: Magnet No	No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No	MAGNO: Magnet No	No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGNO: Magnet No	No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGNO: Magnet No	No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No	MAGNO: Magnet No	No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No	MAGNO: Magnet No	No	No
NOTTITLE1ELIG: Not a Title I School	No	MAGNO: Magnet No	No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No	MAGNO: Magnet No	No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No	MAGNO: Magnet No	No	No

NOTTITLE1ELIG: Not a Title I School	No	MAGNO: Magnet No	No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGNO: Magnet No	No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No	MAGNO: Magnet No	No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGNO: Magnet No	No	No
NOTTITLE1ELIG: Not a Title I School	No	MAGYES: Magnet Yes	No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGNO: Magnet No	No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGNO: Magnet No	No	No
NOTTITLE1ELIG: Not a Title I School	No	MAGNO: Magnet No	No	No
NOTTITLE1ELIG: Not a Title I School	No	MAGNO: Magnet No	No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGNO: Magnet No	No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No	MAGNO: Magnet No	No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGNO: Magnet No	No	No
NOTTITLE1ELIG: Not a Title I School	No	MAGNO: Magnet No	No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No	MAGNO: Magnet No	No	No
NOTTITLE1ELIG: Not a Title I School	No	MAGNO: Magnet No	No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGNO: Magnet No	No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGNO: Magnet No	No	No
NOTTITLE1ELIG: Not a Title I School	No	MAGYES: Magnet Yes	No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGNO: Magnet No	No	No
NOTTITLE1ELIG: Not a Title I School	No	MAGNO: Magnet No	No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGYES: Magnet Yes	No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No	MAGYES: Magnet Yes	No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGNO: Magnet No	No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGNO: Magnet No	No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGNO: Magnet No	No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGNO: Magnet No	No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No	MAGNO: Magnet No	No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No	MAGNO: Magnet No	No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No	MAGNO: Magnet No	No	No

NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No	MAGNO: Magnet No	No	No
NOTTITLE1ELIG: Not a Title I School	No	MAGNO: Magnet No	No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No	MAGNO: Magnet No	No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
NOTTITLE1ELIG: Not a Title I School	No	MAGYES: Magnet Yes	No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGNO: Magnet No	No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGYES: Magnet Yes	No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No	MAGNO: Magnet No	No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGNO: Magnet No	No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGYES: Magnet Yes	No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No	MAGNO: Magnet No	No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGNO: Magnet No	No	Yes
SWELIGNOPROG: Schoolwide Eligible - No Program	No	MAGNO: Magnet No	No	No
NOTTITLE1ELIG: Not a Title I School	No	MAGNO: Magnet No	No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGNO: Magnet No	No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No	MAGNO: Magnet No	No	No
NOTTITLE1ELIG: Not a Title I School	No	MAGNO: Magnet No	No	No
NOTTITLE1ELIG: Not a Title I School	No	MAGYES: Magnet Yes	No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No	MAGNO: Magnet No	No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No	MAGNO: Magnet No	No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No	MAGNO: Magnet No	No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No	MAGYES: Magnet Yes	No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGNO: Magnet No	No	Yes
SWELIGSWPROG: Schoolwide Program	Yes	MAGNO: Magnet No	No	Yes
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No

[illegible]

SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No

SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	Yes
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGNOPROG: Schoolwide Eligible - No Program	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	Yes
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No

SWELIGSWPROG: Schoolwide Program	Yes		No	Yes
SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes		No	No
SWELIGSWPROG: Schoolwide Program	Yes	MAGNO: Magnet No	No	No
NOTTITLE1ELIG: Not a Title I School	No		No	No

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction	KG: Kindergarten	05: Fifth Grade
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
01: Exclusively virtual		
01: Exclusively virtual	KG: Kindergarten	05: Fifth Grade
04: No virtual instruction		

04: No virtual instruction		
04: No virtual instruction	KG: Kindergarten	05: Fifth Grade
04: No virtual instruction	01: First Grade	05: Fifth Grade
04: No virtual instruction	KG: Kindergarten	05: Fifth Grade
04: No virtual instruction	KG: Kindergarten	05: Fifth Grade
04: No virtual instruction	KG: Kindergarten	05: Fifth Grade
04: No virtual instruction	KG: Kindergarten	05: Fifth Grade
04: No virtual instruction	KG: Kindergarten	05: Fifth Grade
04: No virtual instruction		
04: No virtual instruction		
03: Supplemental virtual		
03: Supplemental virtual		
02: Primarily virtual		
03: Supplemental virtual		
01: Exclusively virtual		
02: Primarily virtual	04: Fourth Grade	05: Fifth Grade
03: Supplemental virtual		
04: No virtual instruction		
04: No virtual instruction	KG: Kindergarten	06: Sixth Grade
04: No virtual instruction	KG: Kindergarten	06: Sixth Grade
04: No virtual instruction	KG: Kindergarten	06: Sixth Grade
04: No virtual instruction	KG: Kindergarten	05: Fifth Grade
04: No virtual instruction	KG: Kindergarten	06: Sixth Grade
04: No virtual instruction	KG: Kindergarten	05: Fifth Grade
04: No virtual instruction	KG: Kindergarten	05: Fifth Grade
04: No virtual instruction	KG: Kindergarten	05: Fifth Grade
04: No virtual instruction	KG: Kindergarten	05: Fifth Grade
04: No virtual instruction	KG: Kindergarten	06: Sixth Grade
04: No virtual instruction	KG: Kindergarten	06: Sixth Grade
04: No virtual instruction	KG: Kindergarten	06: Sixth Grade
04: No virtual instruction	KG: Kindergarten	08: Eighth Grade
04: No virtual instruction	KG: Kindergarten	05: Fifth Grade
04: No virtual instruction	KG: Kindergarten	05: Fifth Grade
04: No virtual instruction	KG: Kindergarten	05: Fifth Grade

04: No virtual instruction	06: Sixth Grade	06: Sixth Grade
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
01: Exclusively virtual	KG: Kindergarten	06: Sixth Grade
04: No virtual instruction		
04: No virtual instruction	PK: Pre K	PK: Pre K
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction	KG: Kindergarten	05: Fifth Grade
04: No virtual instruction	KG: Kindergarten	05: Fifth Grade
01: Exclusively virtual		
04: No virtual instruction	KG: Kindergarten	06: Sixth Grade
04: No virtual instruction	KG: Kindergarten	06: Sixth Grade
04: No virtual instruction		
04: No virtual instruction	KG: Kindergarten	05: Fifth Grade
04: No virtual instruction	KG: Kindergarten	05: Fifth Grade
04: No virtual instruction	KG: Kindergarten	05: Fifth Grade
04: No virtual instruction	KG: Kindergarten	05: Fifth Grade
04: No virtual instruction	KG: Kindergarten	06: Sixth Grade
04: No virtual instruction	KG: Kindergarten	06: Sixth Grade
04: No virtual instruction	KG: Kindergarten	06: Sixth Grade
04: No virtual instruction	KG: Kindergarten	06: Sixth Grade
04: No virtual instruction		

04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction	KG: Kindergarten	05: Fifth Grade
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction	KG: Kindergarten	05: Fifth Grade
04: No virtual instruction		
04: No virtual instruction	KG: Kindergarten	05: Fifth Grade
04: No virtual instruction	KG: Kindergarten	06: Sixth Grade
04: No virtual instruction	KG: Kindergarten	06: Sixth Grade
04: No virtual instruction	KG: Kindergarten	06: Sixth Grade
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
03: Supplemental virtual	KG: Kindergarten	06: Sixth Grade
03: Supplemental virtual	KG: Kindergarten	04: Fourth Grade
03: Supplemental virtual	KG: Kindergarten	04: Fourth Grade
03: Supplemental virtual	KG: Kindergarten	04: Fourth Grade
03: Supplemental virtual	KG: Kindergarten	04: Fourth Grade
03: Supplemental virtual		
03: Supplemental virtual	KG: Kindergarten	04: Fourth Grade
03: Supplemental virtual	KG: Kindergarten	06: Sixth Grade
03: Supplemental virtual	KG: Kindergarten	06: Sixth Grade
03: Supplemental virtual		
03: Supplemental virtual	05: Fifth Grade	06: Sixth Grade
03: Supplemental virtual		
03: Supplemental virtual		
03: Supplemental virtual		

03: Supplemental virtual	KG: Kindergarten	06: Sixth Grade
03: Supplemental virtual		
03: Supplemental virtual		
03: Supplemental virtual		
03: Supplemental virtual		
03: Supplemental virtual		
04: No virtual instruction		
01: Exclusively virtual	KG: Kindergarten	06: Sixth Grade
04: No virtual instruction	KG: Kindergarten	06: Sixth Grade
04: No virtual instruction	KG: Kindergarten	06: Sixth Grade
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction	KG: Kindergarten	05: Fifth Grade
04: No virtual instruction	KG: Kindergarten	05: Fifth Grade
04: No virtual instruction	KG: Kindergarten	05: Fifth Grade
04: No virtual instruction	KG: Kindergarten	05: Fifth Grade
04: No virtual instruction	KG: Kindergarten	05: Fifth Grade
04: No virtual instruction	KG: Kindergarten	05: Fifth Grade
04: No virtual instruction	KG: Kindergarten	05: Fifth Grade
04: No virtual instruction		
04: No virtual instruction	KG: Kindergarten	05: Fifth Grade
04: No virtual instruction	KG: Kindergarten	05: Fifth Grade
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
01: Exclusively virtual		

[illegible]

[illegible]

[illegible]

03: Supplemental virtual		
03: Supplemental virtual		
03: Supplemental virtual		
03: Supplemental virtual		
04: No virtual instruction	KG: Kindergarten	05: Fifth Grade
03: Supplemental virtual		
03: Supplemental virtual		
03: Supplemental virtual		
03: Supplemental virtual		
03: Supplemental virtual		
03: Supplemental virtual		
03: Supplemental virtual		
03: Supplemental virtual		
03: Supplemental virtual		
03: Supplemental virtual		
03: Supplemental virtual		
03: Supplemental virtual		
03: Supplemental virtual		
04: No virtual instruction		
03: Supplemental virtual	KG: Kindergarten	05: Fifth Grade
03: Supplemental virtual		
03: Supplemental virtual		
03: Supplemental virtual	KG: Kindergarten	05: Fifth Grade
03: Supplemental virtual		
03: Supplemental virtual		
03: Supplemental virtual		
03: Supplemental virtual		
03: Supplemental virtual		
03: Supplemental virtual		
03: Supplemental virtual		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction	KG: Kindergarten	05: Fifth Grade
03: Supplemental virtual		
03: Supplemental virtual		
04: No virtual instruction		

01: Exclusively virtual	KG: Kindergarten	05: Fifth Grade
04: No virtual instruction		
04: No virtual instruction	KG: Kindergarten	05: Fifth Grade
04: No virtual instruction	03: Third Grade	06: Sixth Grade
03: Supplemental virtual	KG: Kindergarten	05: Fifth Grade
03: Supplemental virtual	KG: Kindergarten	05: Fifth Grade
04: No virtual instruction		
03: Supplemental virtual		
04: No virtual instruction		
04: No virtual instruction		
03: Supplemental virtual		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction	KG: Kindergarten	05: Fifth Grade
04: No virtual instruction	KG: Kindergarten	05: Fifth Grade
04: No virtual instruction	KG: Kindergarten	05: Fifth Grade
04: No virtual instruction	KG: Kindergarten	05: Fifth Grade
04: No virtual instruction	KG: Kindergarten	05: Fifth Grade
04: No virtual instruction	KG: Kindergarten	05: Fifth Grade
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction		
04: No virtual instruction	KG: Kindergarten	05: Fifth Grade
04: No virtual instruction	KG: Kindergarten	05: Fifth Grade

[illegible]

04: No virtual instruction		
04: No virtual instruction	KG: Kindergarten	05: Fifth Grade
04: No virtual instruction	KG: Kindergarten	04: Fourth Grade
04: No virtual instruction	KG: Kindergarten	05: Fifth Grade
04: No virtual instruction		
04: No virtual instruction	KG: Kindergarten	05: Fifth Grade
04: No virtual instruction	KG: Kindergarten	05: Fifth Grade
04: No virtual instruction		
04: No virtual instruction	KG: Kindergarten	05: Fifth Grade
04: No virtual instruction		
04: No virtual instruction	KG: Kindergarten	05: Fifth Grade
	KG: Kindergarten	05: Fifth Grade

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade

[illegible]

07: Seventh Grade	08: Eighth Grade
07: Seventh Grade	08: Eighth Grade
07: Seventh Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
07: Seventh Grade	08: Eighth Grade
07: Seventh Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
07: Seventh Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
07: Seventh Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
07: Seventh Grade	08: Eighth Grade

07: Seventh Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
07: Seventh Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
07: Seventh Grade	08: Eighth Grade
07: Seventh Grade	08: Eighth Grade
05: Fifth Grade	08: Eighth Grade
05: Fifth Grade	08: Eighth Grade
07: Seventh Grade	08: Eighth Grade

06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade

[illegible]

[illegible]

06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade

06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade

06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	06: Sixth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade

06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	06: Sixth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
07: Seventh Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
08: Eighth Grade	08: Eighth Grade
06: Sixth Grade	07: Seventh Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade

06: Sixth Grade	06: Sixth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade
06: Sixth Grade	08: Eighth Grade

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
11: Eleventh Grade	12: Twelfth Grade
11: Eleventh Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
11: Eleventh Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade

09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade

[illegible]

[illegible]

09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade

[illegible]

[illegible]

[illegible]

[illegible]

09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
10: Tenth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade

[illegible]

09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade

09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
11: Eleventh Grade	12: Twelfth Grade
11: Eleventh Grade	12: Twelfth Grade
11: Eleventh Grade	12: Twelfth Grade
11: Eleventh Grade	12: Twelfth Grade
11: Eleventh Grade	12: Twelfth Grade
11: Eleventh Grade	12: Twelfth Grade
11: Eleventh Grade	12: Twelfth Grade
11: Eleventh Grade	12: Twelfth Grade
11: Eleventh Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade

09: Ninth Grade	12: Twelfth Grade
12: Twelfth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	12: Twelfth Grade
09: Ninth Grade	11: Eleventh Grade

Address	City	State	Zip	Physical Address
340 Venturacci Ln	Fallon	NV	89406	340 Venturacci Ln
750 E Williams Ave	Fallon	NV	89406	750 E Williams Ave
1099 Merton Drive	Fallon	NV	89406	1099 Merton Drive
601 Discovery Way	Fallon	NV	89406	601 Discovery Way
650 South Maine Street	Fallon	NV	89406	650 South Maine Street
1 Greenwave Circle	Fallon	NV	89406	1 Greenwave Circle
280 South Russell Street	Fallon	NV	89406	280 South Russell Street
10250 S. El Capitan Way	Las Vegas	NV	89178	10250 S. El Capitan Way
9950 W Tompkins Ave	Las Vegas	NV	89147	9950 W Tompkins Ave
6950 Vegas Valley Dr	Las Vegas	NV	89142	6950 Vegas Valley Dr
3200 Artella Avenue	Henderson	NV	89044	3200 Artella Avenue
10926 Dean Martin Drive	Las Vegas	NV	89141	10926 Dean Martin Drive
2002 Dave Street	Las Vegas	NV	89183	2002 Dave Street
9851 Donald Nelson Ave	Las Vegas	NV	89149	9851 Donald Nelson Avenue
11141 S Pioneer Wy	Las Vegas	NV	89179	11141 S Pioneer Wy
215 Antelope Ridge Dr	Las Vegas	NV	89138	215 Antelope Ridge Dr
9850 Copper Edge Rd	Las Vegas	NV	89148	9850 Copper Edge Rd
550 Dave Wood Circle	Henderson	NV	89011	550 Dave Wood Circle
7950 Arville St	Las Vegas	NV	89139	7950 Arville St
4497 Kell Ln	Las Vegas	NV	89110	4497 Kell Ln
8951 W Ford Ave	Las Vegas	NV	89148	8951 W Ford Ave
8200 W Tropical Pkwy	Las Vegas	NV	89149	8200 W Tropical Pkwy
250 W Rome Blvd	N Las Vegas	NV	89084	250 W Rome Blvd
2333 Canyon Retreat Dr	Henderson	NV	89044	2333 Canyon Retreat Dr
4905 Chartan Ave	Las Vegas	NV	89141	4905 Chartan Ave
5445 Cedar Ave	Las Vegas	NV	89110	5445 Cedar Ave
6635 W Cougar Ave	Las Vegas	NV	89139	6635 W Cougar Ave
7431 Egan Crest Dr	Las Vegas	NV	89149	7431 Egan Crest Dr
4470 W Rome Blvd	N Las Vegas	NV	89084	4470 W Rome Blvd
8455 O'Hare Road	Las Vegas	NV	89143	8455 O'Hare Road
10025 Rumrill St	Las Vegas	NV	89178	10025 Rumrill St
4450 E Owens Ave	Las Vegas	NV	89115	4450 E Owens Ave
5700 N Bruce St	N Las Vegas	NV	89081	5700 N Bruce St
5710 Mountain Vista St.	Las Vegas	NV	89120	5710 Mountain Vista St.

1950 Pink Rose St.	Las Vegas	NV	89106	1950 Pink Rose St.
304 E Paradise Hills Dr	Henderson	NV	89002	304 E Paradise Hills Dr
3700 Shadow Tree St	N Las Vegas	NV	89032	3700 Shadow Tree St
5550 Milan Peak St	N Las Vegas	NV	89081	5550 Milan Peak St
4525 Jimmy Durante Blvd	Las Vegas	NV	89122	4525 Jimmy Durante Blvd
2755 Mohawk St	Las Vegas	NV	89146	2755 Mohawk St
8601 S Grand Canyon Dr	Las Vegas	NV	89178	8601 S Grand Canyon Dr
6995 W Eldorado Ln	Las Vegas	NV	89113	6995 W Eldorado Ln
11420 Placid Street	Las Vegas	NV	89183	11420 Placid Street
5555 Horse Drive	Las Vegas	NV	89131	5555 Horse Drive
6 Diamond St	Blue Diamond	NV	89004	6 Diamond St
4405 Yellow Pine Ave	Mt Charleston	NV	89124	4405 Yellow Pine Ave
300 Michael Wendell Way	Searchlight	NV	89046	300 Michael Wendell Way
2260 Betty Ln	Las Vegas	NV	89156	2260 Betty Ln
4550 N Pioneer Way	Las Vegas	NV	89129	4550 N Pioneer Way
7600 Peace Way	Las Vegas	NV	89147	7600 Peace Way
8685 Hidden Palms Pkwy	Las Vegas	NV	89123	8685 Hidden Palms Pkwy
9001 Mariner Cove Dr	Las Vegas	NV	89117	9001 Mariner Cove Dr
4100 Thom Blvd	Las Vegas	NV	89130	4100 Thom Blvd
1940 Chickasaw Dr	Henderson	NV	89002	1940 Chickasaw Dr
2000 S Sloan Ln	Las Vegas	NV	89142	2000 S Sloan Ln
7000 Walt Lott Dr	Las Vegas	NV	89128	7000 Walt Lott Dr
1255 Patriots Way	Moapa	NV	89025	1255 Patriots Way
4850 Kell Ln	Las Vegas	NV	89115	4850 Kell Ln
3955 Timberlake Dr	Las Vegas	NV	89115	3955 Timberlake Dr
2701 Harris St	Las Vegas	NV	89101	2701 Harris St
7770 Delhi Ave	Las Vegas	NV	89129	7770 Delhi Ave
2200 James Bilbray Dr	Las Vegas	NV	89108	2200 James Bilbray Dr
271 Leisure Cir	Henderson	NV	89074	271 Leisure Cir
5655 Edna Ave	Las Vegas	NV	89146	5655 Edna Ave
560 E Eldorado Ln	Las Vegas	NV	89123	560 E Eldorado Ln
8400 Boseck Dr	Las Vegas	NV	89145	8400 Boseck Dr
1900 S Lisa Ln	Las Vegas	NV	89117	1900 S Lisa Ln
4145 Jimmy Durante	Las Vegas	NV	89122	4145 Jimmy Durante
280 Clark Dr	Henderson	NV	89074	280 Clark Dr

1698 Patrick Ln	Henderson	NV	89014	1698 Patrick Ln
425 N Christy Ln	Las Vegas	NV	89110	425 N Christy Ln
6475 Eagle Creek Ln	Las Vegas	NV	89156	6475 Eagle Creek Ln
2001 E Reno Ave	Las Vegas	NV	89119	2001 E Reno Ave
580 N Fogg St	Las Vegas	NV	89110	580 N Fogg St
6350 W Washburn Rd	Las Vegas	NV	89130	6350 W Washburn Rd
7887 W Gowan Rd	Las Vegas	NV	89129	7887 W Gowan Rd
1800 Rock Springs Dr	Las Vegas	NV	89128	1800 Rock Springs Dr
5150 Duneville St	Las Vegas	NV	89118	5150 Duneville St
888 Adams Blvd	Boulder City	NV	89005	888 Adams Blvd
1961 Wigwam Pkwy	Henderson	NV	89074	1961 Wigwam Pkwy
3550 S Kevin Way	Las Vegas	NV	89147	3550 S Kevin Way
1650 Patrick Ln	Henderson	NV	89014	1650 Patrick Ln
1101 W Tropical Pkwy	N Las Vegas	NV	89031	1101 W Tropical Pkwy
9000 Hillpointe Rd	Las Vegas	NV	89134	9000 Hillpointe Rd
450 E Eldorado Ln	Las Vegas	NV	89123	450 E Eldorado Ln
2651 N Revere St	N Las Vegas	NV	89030	2651 N Revere St
4225 N Lamont St	Las Vegas	NV	89115	4225 N Lamont St
9601 Red Hills Rd	Las Vegas	NV	89117	9601 Red Hills Rd
571 Greenway Rd	Henderson	NV	89015	571 Greenway Rd
4289 Allen Ln	N Las Vegas	NV	89032	4289 Allen Ln
8050 Cielo Vista Ave	Las Vegas	NV	89128	8050 Cielo Vista Ave
609 W Alexander Rd	N Las Vegas	NV	89032	609 W Alexander Rd
227 Charter Oak St	Henderson	NV	89074	227 Charter Oak St
8680 W Hammer Ln	Las Vegas	NV	89149	8680 W Hammer Ln
4027 W Washburn Rd	N Las Vegas	NV	89031	4027 W Washburn Rd
1651 Orchard Valley Dr	Las Vegas	NV	89142	1651 Orchard Valley Dr
2040 Desert Shadow Trail	Henderson	NV	89012	2040 Desert Shadow Trail
2851 Harris Ave	Las Vegas	NV	89101	2851 E Harris Ave
8255 Katie Ave	Las Vegas	NV	89147	8255 Katie Ave
765 Crestdale Ln	Las Vegas	NV	89144	765 Crestdale Ln
1050 E Gary Ave	Las Vegas	NV	89123	1050 E Gary Ave
451 Vincen Leavitt Ave	Bunkerville	NV	89007	451 Vincen Leavitt Ave
7350 Tealwood St	Las Vegas	NV	89131	7350 Tealwood St
4028 La Madre Way	N Las Vegas	NV	89031	4028 La Madre Way

1070 Featherwood Ave	Henderson	NV	89015	1070 Featherwood Ave
6350 Peak Dr	Las Vegas	NV	89108	6350 Peak Dr
4865 Goldfield St	N Las Vegas	NV	89031	4865 Goldfield St
4245 E Tonopah Ave	Las Vegas	NV	89115	4245 E Tonopah Ave
2551 Summit Grove Dr	Henderson	NV	89052	2551 Summit Grove Dr
3850 Campbell Rd	Las Vegas	NV	89129	3850 Campbell Rd
9620 W Twain Ave	Las Vegas	NV	89147	9620 W Twain Ave
231 Bailey Island Dr	Henderson	NV	89074	231 Bailey Island Dr
6651 W Azure Drive	Las Vegas	NV	89130	6651 W Azure Drive
5625 Corbett St	Las Vegas	NV	89130	5625 Corbett St
9480 W Tropical Pkwy	Las Vegas	NV	89149	9480 W Tropical Pkwy
5150 Whispering Sands Dr	Las Vegas	NV	89131	5150 Whispering Sands Dr
5535 S Riley St	Las Vegas	NV	89148	5535 S Riley St
4317 E Colorado Ave	Las Vegas	NV	89104	4317 E Colorado Ave
2060 Desert Shadow Trail	Henderson	NV	89012	2060 Desert Shadow Trail
5845 N Commerce St	N Las Vegas	NV	89031	5845 N Commerce St
7455 El Camino Rd	Las Vegas	NV	89139	7455 El Camino Rd
6225 E Washington Ave	Las Vegas	NV	89110	6225 E Washington Ave
5335 Coleman Street	N Las Vegas	NV	89031	5335 Coleman Street
1155 E Richmar Ave	Las Vegas	NV	89123	1155 E Richmar Ave
1575 S Hollywood Blvd	Las Vegas	NV	89142	1575 S Hollywood Blvd
850 Scholar St	Henderson	NV	89002	850 Scholar St
3810 Shadow Peak Dr	Las Vegas	NV	89129	3810 Shadow Peak Dr
655 Park Vista Dr	Las Vegas	NV	89138	655 Park Vista Dr
11175 W Desert Inn Rd	Las Vegas	NV	89135	11175 W Desert Inn Rd
9800 Placid St	Las Vegas	NV	89183	9800 Placid St
9371 Iron Mountain Rd	Las Vegas	NV	89143	9371 Iron Mountain Rd
2328 Silver Clouds Dr	N Las Vegas	NV	89031	2328 Silver Clouds Dr
9135 W Maule Ave	Las Vegas	NV	89148	9135 W Maule Ave
3030 E Tropical Pkwy	N Las Vegas	NV	89081	3030 E Tropical Pkwy
5700 W Harmon Ave	Las Vegas	NV	89103	5700 W Harmon Ave
10135 W Quail Ave	Las Vegas	NV	89148	10135 W Quail Ave
9805 S Lindell Rd	Las Vegas	NV	89141	9805 S Lindell Rd
2450 N Hollywood Blvd	Las Vegas	NV	89156	2450 N Hollywood Blvd
2320 Clifford St	Las Vegas	NV	89115	2320 Clifford St

3409 Deer Springs Way	N Las Vegas	NV	89084	3409 Deer Springs Way
7351 N Campbell Road	Las Vegas	NV	89149	7351 N Campbell Road
150 W Rome Blvd	N Las Vegas	NV	89084	150 W Rome Blvd
8425 Bob Fisk Avenue	Las Vegas	NV	89178	8425 Bob Fisk Avenue
5701 Stacey Ave	Las Vegas	NV	89108	5701 Stacey Ave
950 N Tonopah Dr	Las Vegas	NV	89106	950 N Tonopah Dr
1100 Lena St	Las Vegas	NV	89101	1100 Lena St
1312 E Tonopah Ave	N Las Vegas	NV	89030	1312 E Tonopah Ave
1300 Pauline Way	Las Vegas	NV	89104	1300 Pauline Way
2101 W Cartier Ave	N Las Vegas	NV	89032	2101 W Cartier Ave
1750 Lindell Rd	Las Vegas	NV	89146	1750 Lindell Rd
324 Essex Dr	Las Vegas	NV	89107	324 Essex Dr
2421 N Kenneth	N Las Vegas	NV	89030	2421 N Kenneth
701 N 20th St	Las Vegas	NV	89101	701 N 20th St
2277 N MLK Blvd	Las Vegas	NV	89106	2277 N MLK Blvd
4620 E. Monroe Ave.	Las Vegas	NV	89110	4620 E. Monroe Ave.
4351 Lamont St	Las Vegas	NV	89115	4351 Lamont St
4869 E Sun Valley Dr	Las Vegas	NV	89121	4869 E Sun Valley Dr
3840 Pecos McLeod Interconnect	Las Vegas	NV	89121	3840 Pecos McLeod Interconnect
931 Franklin Ave	Las Vegas	NV	89104	931 Franklin Ave
2726 Englestad	N Las Vegas	NV	89030	2726 Englestad
1315 Hiawatha Rd	Las Vegas	NV	89108	1315 Hiawatha Rd
1735 D St	Las Vegas	NV	89106	1735 D St
3046 Ferndale St.	Las Vegas	NV	89121	3046 Ferndale St.
4338 S Bruce St	Las Vegas	NV	89119	4338 S Bruce St
3010 Berg St	N Las Vegas	NV	89030	3010 Berg St
2637 E Gowan Rd	N Las Vegas	NV	89030	2637 E Gowan Rd
1030 J St	Las Vegas	NV	89106	1030 J St
2801 Ft Sumter Dr	N Las Vegas	NV	89030	2801 Ft Sumter Dr
4101 West Bonanza Road	Las Vegas	NV	89106	1900 J St
3656 SX. Pecos-McLeod Interconnect	Las Vegas	NV	89121	3656 S. Pecos-McLeod Interconnect
1810 Shaner Ln	Las Vegas	NV	89156	1810 Shaner Ln
2655 Siena Heights Dr	Henderson	NV	89052	2655 Siena Heights Dr
6350 Hyde Ave	Las Vegas	NV	89107	6350 Hyde Ave
900 Cottage Grove Ave	Las Vegas	NV	89119	900 Cottage Grove Ave

1200 N Mallard	Las Vegas	NV	89108	1200 N Mallard
800 E Carey Ave	N Las Vegas	NV	89030	800 E Carey Ave
408 Upland Blvd	Las Vegas	NV	89107	408 Upland Blvd
2900 Wilmington Way	Las Vegas	NV	89102	2900 Wilmington Way
2904 Meteoro St	Las Vegas	NV	89169	2904 Meteoro St
6451 Brandywine Way	Las Vegas	NV	89107	6451 Brandywine Way
1560 Cherokee Ln	Las Vegas	NV	89169	1560 E Cherokee Ln
211 28th Street	Las Vegas	NV	89101	211 28th Street
3000 E Tonopah Ave	N Las Vegas	NV	89030	3000 E Tonopah Ave
1205 Silver Lake Drive	Las Vegas	NV	89108	1205 Silver Lake Drive
6333 Fargo Ave	Las Vegas	NV	89107	6333 Fargo Ave
4000 El Parque Ave	Las Vegas	NV	89102	4000 El Parque Ave
2712 Searles Ave.	Las Vegas	NV	89101	2712 Searles Ave.
2831 Palomino Ln	Las Vegas	NV	89107	2831 Palomino Ln
3223 S Glenhurst	Las Vegas	NV	89121	3223 S Glenhurst
330 Tin Street	Henderson	NV	89015	330 Tin Street
900 Ave B	Boulder City	NV	89005	900 Ave B
700 E Lake Mead Dr	Henderson	NV	89015	700 E Lake Mead Dr
400 Sky Rd	Indian Springs	NV	89018	400 Sky Rd
4150 Fuselier Dr	N Las Vegas	NV	89032	4150 Fuselier Dr
144 Westminster Way	Henderson	NV	89015	144 Westminster Way
200 Woodbury Ln	Mesquite	NV	89027	200 Woodbury Ln
5005 Keenan Ave	Las Vegas	NV	89122	5005 Keenan Ave
4225 El Oro Street	Las Vegas	NV	89121	4225 El Oro Street
1555 E Hacienda Ave	Las Vegas	NV	89119	1555 E Hacienda Ave
2001 Winterwood Blvd.	Las Vegas	NV	89142	2001 Winterwood Blvd.
4150 East Carey Ave	Las Vegas	NV	89115	4150 East Carey Ave
4820 E. MESA VISTA AVENUE	Las Vegas	NV	89120	4820 E. MESA VISTA AVENUE
3850 E. Twain Ave	Las Vegas	NV	89121	3850 E. Twain Ave
4220 S Ravenwood	Las Vegas	NV	89147	4220 S Ravenwood
7101 Pinedale Ave.	Las Vegas	NV	89145	7101 Pinedale Ave.
5445 S Annie Oakley Dr	Las Vegas	NV	89120	5445 S Annie Oakley Dr
4450 S Ridgeville St	Las Vegas	NV	89103	4450 S Ridgeville St
4551 Diamond Head	Las Vegas	NV	89110	4551 Diamond Head
3235 E Hacienda	Las Vegas	NV	89120	3235 E Hacienda

3850 S Redwood	Las Vegas	NV	89103	3850 S Redwood
2000 S Walnut Rd	Las Vegas	NV	89104	2000 S Walnut Rd
9370 Brent Ln	Las Vegas	NV	89143	9370 Brent Ln
5800 Broken Top Ave	Las Vegas	NV	89141	5800 Broken Top Ave
1776 East Ogden Ave	Las Vegas	NV	89101	1776 East Ogden Ave
4851 E Lake Mead Blvd	Las Vegas	NV	89115	4851 E Lake Mead Blvd
555 N Honolulu	Las Vegas	NV	89110	555 N Honolulu
701 Skyline Rd	Henderson	NV	89002	701 Skyline Rd
3170 Laurel Ave	Henderson	NV	89014	3170 Laurel Ave
2825 S Torrey Pines Dr	Las Vegas	NV	89146	2825 S Torrey Pines Dr
1415 W Whipple Rd	Logandale	NV	89021	1415 W Whipple Rd
10377 Rancho Destino Rd	Las Vegas	NV	89183	10377 Rancho Destino Rd
350 E Judson Ave	N Las Vegas	NV	89030	350 E Judson Ave
491 N Lamb Blvd	Las Vegas	NV	89110	491 N Lamb Blvd
3035 Desert Marigold Ln	Las Vegas	NV	89135	3035 Desert Marigold Ln
5150 E Desert Inn Rd	Las Vegas	NV	89122	5150 E Desert Inn Rd
9400 W Gilmore Ave	Las Vegas	NV	89129	9400 W Gilmore Ave
1700 Sageberry Dr	Las Vegas	NV	89144	1700 Sageberry Dr
1001 Seven Hills Dr	Henderson	NV	89052	1001 Seven Hills Dr
3650 Cambridge St	Las Vegas	NV	89169	3650 Cambridge St
6510 Buckskin Ave	Las Vegas	NV	89108	6510 Buckskin Ave
1420 E. Pearl Ave.	Sandy Valley	NV	89019	1420 E. Pearl Ave.
1450 Spirit Lane	Laughlin	NV	89029	1450 Spirit Lane
3855 Timberlake Dr	Las Vegas	NV	89115	3855 Timberlake Dr
5350 Harris Ave	Las Vegas	NV	89110	5350 Harris Ave
2501 Winwood St	Las Vegas	NV	89108	2501 Winwood St
6650 W Reno Ave	Las Vegas	NV	89118	6650 W Reno Ave
450 Merlayne Dr	Henderson	NV	89011	450 Merlayne Dr
1831 Fox Ridge Dr	Henderson	NV	89014	1831 Fox Ridge Dr
1960 Ferrell St	Las Vegas	NV	89106	1960 Ferrell St
2436 N Pecos Rd	Las Vegas	NV	89115	2436 N Pecos Rd
6371 Hyde Ave	Las Vegas	NV	89107	6371 Hyde Ave
900 Hinson St	Las Vegas	NV	89107	900 Hinson St
4622 W Desert Inn Rd	Las Vegas	NV	89102	4622 W Desert Inn Rd
1880 E Stanley Ave	N Las Vegas	NV	89030	1880 E Stanley Ave

2422 Maverick St	Las Vegas	NV	89108	2422 Maverick St
2505 N Bruce St	N Las Vegas	NV	89030	2505 N Bruce St
1100 E St Louis Ave	Las Vegas	NV	89104	1100 E St Louis Ave
2400 Atlantic St	Las Vegas	NV	89104	2400 Atlantic St
3900 W Washington Ave	Las Vegas	NV	89107	3900 W Washington Ave
200 N 28th Street	Las Vegas	NV	89101	200 N 28th Street
1562 E Katie Ave	Las Vegas	NV	89119	1562 E Katie Ave
355 W Van Wagenen	Henderson	NV	89015	355 W Van Wagenen
3875 E Harmon Ave	Las Vegas	NV	89121	3875 E Harmon Ave
5850 Euclid Ave	Las Vegas	NV	89120	5850 Euclid Ave
4150 S Torrey Pines Dr	Las Vegas	NV	89103	4150 S Torrey Pines Dr
1200 Ave G	Boulder City	NV	89005	1200 Ave G
307 Cannes St	Henderson	NV	89015	307 Cannes St
1420 E. Pearl Ave.	Sandy Valley	NV	89019	1420 E. Pearl Ave.
1900 Cougar Dr	Laughlin	NV	89029	1900 Cougar Dr
1450 Radwick Dr	Las Vegas	NV	89110	1450 Radwick Dr
7701 Ducharme Ave	Las Vegas	NV	89145	7701 Ducharme Ave
140 N Valle Verde	Henderson	NV	89074	140 N Valle Verde
3500 W Gilmore Ave	N Las Vegas	NV	89032	3500 W Gilmore Ave
1661 Galleria Dr	Henderson	NV	89014	1661 Galleria Dr
9151 Pinewood Hills Dr	Las Vegas	NV	89134	9151 Pinewood Hills Dr
5450 Redwood St	Las Vegas	NV	89118	5450 Redwood St
179 S Andersen	Overton	NV	89040	179 S Andersen
2050 Sapphire Stone Ave	Las Vegas	NV	89106	2050 Sapphire Stone Ave
5350 W Tropical Pkwy	Las Vegas	NV	89130	5350 W Tropical Pkwy
301 N Fogg St	Las Vegas	NV	89110	301 N Fogg St
7801 W Gilmore Ave	Las Vegas	NV	89129	7801 W Gilmore Ave
1055 Silverado Ranch Blvd	Las Vegas	NV	89123	1055 Silverado Ranch Blvd
5301 E Hacienda Ave	Las Vegas	NV	89122	5301 E Hacienda Ave
400 Sky Rd	Indian Springs	NV	89018	400 Sky Rd
4410 S Juliano Rd	Las Vegas	NV	89147	4410 S Juliano Rd
2400 Cozy Hill Cir	Henderson	NV	89052	2400 Cozy Hill Cir
235 N Pavilion Center Dr	Las Vegas	NV	89144	235 N Pavilion Center Dr
4701 Quadrel St	Las Vegas	NV	89129	4701 Quadrel St
1900 W Deer Springs Way	N Las Vegas	NV	89084	1900 W Deer Springs Way

1870 N Lamont St	Las Vegas	NV	89115	1870 N Lamont St
8625 Spencer St	Las Vegas	NV	89123	8625 Spencer St
3465 Englestad St	N Las Vegas	NV	89032	3465 Englestad St
1580 S Hollywood Blvd	Las Vegas	NV	89142	1580 S Hollywood Blvd
9905 W Mesa Vista Ave	Las Vegas	NV	89148	9905 W Mesa Vista Ave
7775 Elkhorn Rd	Las Vegas	NV	89131	7775 Elkhorn Rd
7808 S Torrey Pines Dr	Las Vegas	NV	89139	7808 S Torrey Pines Dr
550 Hafen Ln	Mesquite	NV	89027	550 Hafen Ln
333 W Tropical Pkwy	N Las Vegas	NV	89031	333 W Tropical Pkwy
155 E Paradise Hills Dr	Henderson	NV	89002	155 E Paradise Hills Dr
8101 N Torrey Pines Dr	Las Vegas	NV	89131	8101 N Torrey Pines Dr
2200 Reunion Dr	Henderson	NV	89052	2200 Reunion Dr
4250 Karen Ave	Las Vegas	NV	89121	4250 Karen Ave
2500 N Hollywood Blvd	Las Vegas	NV	89156	2500 N Hollywood Blvd
5855 Lawrence Street	N Las Vegas	NV	89081	5855 Lawrence Street
5800 W Pyle Avenue	Las Vegas	NV	89141	5800 W Pyle Avenue
9501 Echelon Point Dr	Las Vegas	NV	89149	9501 Echelon Point Dr
9525 W Maule Ave	Las Vegas	NV	89148	9525 W Maule Ave
10155 Marnie St	Las Vegas	NV	89178	10155 Marnie St
2726 ENGLESTAD STREET	NORTH LAS VEGAS	NV	89030	2726 ENGLESTAD STREET
4291 W Pennwood Ave	Las Vegas	NV	89102	4291 W Pennwood Ave
6500 E Sahara Ave	Las Vegas	NV	89142	6500 E Sahara Ave
1900 Searles Avenue	Las Vegas	NV	89101	1900 Searles Avenue
2839 S Burnham Ave	Las Vegas	NV	89169	2839 S Burnham Ave
4601 W Bonanza Rd	Las Vegas	NV	89107	4601 W Bonanza Rd
400 Palo Verde Dr	Henderson	NV	89015	400 Palo Verde Dr
3801 E Washington Ave	Las Vegas	NV	89110	3801 E Washington Ave
3850 Annie Oakley Dr	Las Vegas	NV	89121	3850 Annie Oakley Dr
1139 N Linn Ln	Las Vegas	NV	89110	1139 N Linn Ln
6665 W Del Rey Avenue	Las Vegas	NV	89146	6665 W Del Rey
5710 Mountain Vista	Las Vegas	NV	89120	5710 Mountain Vista
2301 N Tenaya Way	Las Vegas	NV	89128	2301 N Tenaya Way
3200 W Alexander Rd	N Las Vegas	NV	89032	3200 W Alexander Rd
460 North Arroyo Grande Blvd	Henderson	NV	89014	460 Arroyo Grande Blvd
7100 W Dewey Dr	Las Vegas	NV	89113	7100 W Dewey Dr

315 S 7th St	Las Vegas	NV	89101	315 S 7th St
1411 Robin Street	Las Vegas	NV	89106	1411 Robin Street
1650 Silver Hawk Ave	Las Vegas	NV	89123	1650 Silver Hawk Ave
3200 E Cheyenne Ave	N Las Vegas	NV	89030	3200 E Cheyenne Ave
6375 W Charleston Blvd	Las Vegas	NV	89146	6375 W Charleston Blvd
5302 Goldfield St	N Las Vegas	NV	89031	5302 Goldfield St
333 S Pavilion Center Dr	Las Vegas	NV	89144	333 S Pavilion Center Dr
700 College Dr	Henderson	NV	89002	700 College Dr
5050 Brent Ln	Las Vegas	NV	89131	5050 Brent Ln
3700 Liberty Heights Ave	Henderson	NV	89052	3700 Liberty Heights Ave
350 E Alexander Rd	N Las Vegas	NV	89032	350 E Alexander Rd
3100 E Patrick Ln	Las Vegas	NV	89120	3100 E Patrick Ln
3750 S Buffalo Dr	Las Vegas	NV	89147	3750 S Buffalo Dr
2531 Vegas Dr	Las Vegas	NV	89106	2531 Vegas Dr
7050 W Shelbourne Ave	Las Vegas	NV	89113	7050 W Shelbourne Ave
2575 N Los Feliz St	Las Vegas	NV	89156	2575 N Los Feliz St
11945 W Charleston Blvd	Las Vegas	NV	89135	11945 W Charleston Blvd
10 CHAPATA DRIVE	Henderson	NV	89012	10 CHAPATA DRIVE
1101 Fifth St	Boulder City	NV	89005	1101 Fifth St
2400 St Joseph St	Overton	NV	89040	2400 St Joseph St
820 Valley View Dr	Mesquite	NV	89027	820 Valley View Dr
400 Sky Road	Indian Springs	NV	89018	400 Sky Road
10200 Centennial Pkwy	Las Vegas	NV	89149	10200 Centennial Pkwy
800 College Dr	Henderson	NV	89002	800 College Dr
3800 Harris Ave	Las Vegas	NV	89110	3800 Harris Ave
8100 W Robindale Rd	Las Vegas	NV	89113	8100 W Robindale Rd
1001 Coronado Center Dr	Henderson	NV	89052	1001 Coronado Center Dr
7500 Whispering Sands D	Las Vegas	NV	89131	7500 Whispering Sands D
150 W Deer Springs Way	N Las Vegas	NV	89084	150 W Deer Springs Way
8200 W Tropical Pkwy	Las Vegas	NV	89149	8200 W Tropical Pkwy
6600 W Erie Ave	Las Vegas	NV	89141	6600 W Erie Ave
6705 Vegas Valley Dr	Las Vegas	NV	89142	6705 Vegas Valley Dr
3050 E Flamingo Rd	Las Vegas	NV	89121	3050 E Flamingo Rd
3050 E. FLAMINGO ROAD	Las Vegas	NV	89121	3050 E. FLAMINGO ROAD
1725 S. Maryland Pkwy	Las Vegas	NV	89104	1725 S. Maryland Pkwy

405 W. Dorrell Lane	North Las Vegas	NV	89084	405 W. Dorrell Lane
4250 E Bonanza Rd, Suite 10	Las Vegas	NV	89110	2020 W. Craig Road Suite 301
601 N Pecos Rd Suite 70	Las Vegas	NV	89101	601 N Pecos Rd Suite 70
405 W. Dorrell Lane	North Las Vegas	NV	89084	405 W. Dorrell Lane
225 E. Starr Ave	Las Vegas	NV	89183	225 E. Starr Ave
3200 W. Alexander Road	North Las Vegas	NV	89032	3200 W. Alexander Road
2301 N. Tenaya Way	Las Vegas	NV	89128	2301 N. Tenaya Way
3800 Harris Avenue	Las Vegas	NV	89110	3800 Harris Avenue
4601 W. Bonanza Rd	Las Vegas	NV	89107	4601 W. Bonanza Rd
6665 W. Del Ray Ave	Las Vegas	NV	89146	6665 W. Del Ray Ave
2375 E Viking	Las Vegas	NV	89169	2375 E Viking
2800 E Stewart Ave	Las Vegas	NV	89101	2800 E Stewart Ave
601 N Pecos Rd Suite 70	Las Vegas	NV	89101	601 N Pecos Rd Suite 70
SR 89038 PO Box 252	Las Vegas	NV	89115	SR 89038 PO Box 252
245 N Pecos	Las Vegas	NV	89101	245 N Pecos
245 N Pecos	Las Vegas	NV	89101	245 N Pecos
5730 Range Rd	Las Vegas	NV	89115	5730 Range Rd
4560 W Harmon Ave	Las Vegas	NV	89103	4560 W Harmon Ave
1725 S MARYLAND PARKWAY	Las Vegas	NV	89104	1725 S MARYLAND PARKWAY
5300 E Russell Rd	Las Vegas	NV	89122	5300 E Russell Rd
245 N Pecos	Las Vegas	NV	89101	245 N Pecos
245 N Pecos	Las Vegas	NV	89101	245 N Pecos
4560 W Harmon Ave	Las Vegas	NV	89103	4560 W Harmon Ave
5300 E Russell Rd	Las Vegas	NV	89122	5300 E Russell Rd
10250 W Centennial Pkwy	Las Vegas	NV	89149	10250 W Centennial Pkwy
2800 E Stewart Ave	Las Vegas	NV	89101	2800 E Stewart Ave
601 N Pecos Rd Suite 70	Las Vegas	NV	89101	601 N Pecos Rd Suite 70
601 N Pecos Rd Suite 70	Las Vegas	NV	89101	601 N Pecos Rd Suite 70
22010 Cold Creek Rd	Indian Springs	NV	89070	22010 Cold Creek Rd
2701 E St Louis Ave	Las Vegas	NV	89104	2701 E. St. Louis Ave
20825 Cold Creek Rd	Indian Springs	NV	89070	20825 Cold Creek Rd
4370 Smiley Rd	N Las Vegas	NV	89115	4370 Smiley Rd
444 W Brooks Ave	N Las Vegas	NV	89030	444 W Brooks Ave
22010 Cold Creek Rd	Indian Springs	NV	89018	22010 Cold Creek Rd
801 Veterans Memorial Drive	Las Vegas	NV	89101	801 Veterans Memorial Drive

115 Healing Center Drive	Boulder City	NV	89005	115 Healing Center Drive
3626 S Pecos-McLeod	Las Vegas	NV	89121	3626 S Pecos-McLeod
601 N Pecos Rd Suite 70	Las Vegas	NV	89101	601 N Pecos Rd Suite 70
1290 Toler Avenue	Gardnerville	NV	89410	1290 Toler Avenue
PO Box 7	Zephyr Cove	NV	89448	226 Warrior Way
701 Jacks Valley Road	Carson City	NV	89705	701 Jacks Valley Road
699 Long Valley Rd	Gardnerville	NV	89460	699 Long Valley Rd
1479 Stephanie Way	Minden	NV	89423	1479 Stephanie Way
1170 Baler Street	Minden	NV	89423	1170 Baler Street
1477 Hwy 395	Gardnerville	NV	89410	1477 Hwy 395
701 Long Valley Rd	Gardnerville	NV	89460	701 Long Valley Rd
1670 Hwy 88	Minden	NV	89423	1670 Hwy 88
PO Box 677	Zephyr Cove	NV	89448	240 Warrior Way
225 China Spring Rd	Gardnerville	NV	89410	225 China Spring Rd
1286 Toler Avenue	Gardnerville	NV	89410	1286 Toler Avenue
1286 Toler Ave	Gardnerville	NV	89410	1286 Toler Ave
1670 HWY 88	Minden	NV	89423	1670 HWY 88
1286 Toler Avenue	Gardnerville	NV	89410	1286 Toler Avenue
1638 Mono Avenue	Minden	NV	89423	1638 Mono Avenue
HC 32 Box 110	Tuscarora	NV	89834	1645 Sewell Drive
PO Box 463	Jackpot	NV	89825-0463	2201 Progressive Drive
PO Box 597	Montello	NV	89830	254 B Street
HC 30 Box 348	Jiggs	NV	89815	208 Boyd Kennedy Road
HC 60 Box 620	Ruby Valley	NV	89833	1129 Lake Avenue
250 Parkchester Drive	Spring Creek	NV	89815	250 Parkchester Drive
1055 7th Street	Elko	NV	89801	1055 7th Street
1645 Sewell Drive	Elko	NV	89801-2847	1645 Sewell Drive
501 South 9th Street	Elko	NV	89801-3326	501 South 9th Street
PO Box 730	Carlin	NV	89822-0729	552 8th Street
PO Box 100	Owyhee	NV	89832	100 Academic Way
PO Box 338	Wells	NV	89835-0338	1378 Lake Avenue
PO Box 2400	West Wendover	NV	89883-2400	2332 Florence Way
3300 Argent Avenue	Elko	NV	89801-4414	3300 Argent Avenue
7 East Licht Parkway	Spring Creek	NV	89815	7 East Licht Parkway
208 Boyd-Kennedy Road	Spring Creek	NV	89815	208 Boyd-Kennedy Road

777 Country Club Dr	Elko	NV	89801	777 Country Club Dr
PO Box 730	Carlin	NV	89822-0729	552 8th Street
PO Box 338	Wells	NV	89835-0338	1129 Lake Avenue
3375 Jennings Way	Elko	NV	89801-2677	3375 Jennings Way
14650 Lamoille Highway	Spring Creek	NV	89815	14650 Lamoille Highway
PO Box 463	Jackpot	NV	89825-0463	2201 Progressive Drive
PO Box 100	Owyhee	NV	89832	100 Academic Way
PO Box 5100	West Wendover	NV	89883-2400	2000 Elko Avenue
PO Box 730	Carlin	NV	89822-0729	552 8th Street
PO Box 338	Wells	NV	89835-0338	1129 Lake Avenue
987 College Avenue	Elko	NV	89801-3419	987 College Avenue
PO Box 100	Owyhee	NV	89832	100 Academic Way
PO Box 463	Jackpot	NV	89825-0463	2201 Progressive Drive
14550 Lamoille Highway	Spring Creek	NV	89815	14550 Lamoille Highway
PO Box 3830	West Wendover	NV	89883-2400	2055 Elko Avenue
850 Elm Street	Elko	NV	89801	850 Elm Street
850 Elm Street	Elko	NV	89801	850 Elm Street
850 Elm Street	Elko	NV	89801	850 Elm Street
850 Elm Street	Elko	NV	89801	850 Elm Street
P.O. Box 700	Carlin	NV	89822	100 University Ave
PO. Box 129	Dyer	NV	89010	Hwy 264 MM 11
PO. Box 129	Dyer	NV	89010	5th & Ramsey
PO Box 129	Dyer	NV	89010	MM11 Hwy 264
444 4th Street	Crescent Valley	NV	89821	444 4th Street
PO Box 249	Eureka	NV	89316	431 McCoy Street
PO Box 237	Eureka	NV	89316	1 Vandal Way
PO Box 76	Denio	NV	89404-0076	130 Juniper Dr. / PO Box 76
134 Kings River Road	Kings River	NV	89425	134 Kings River Road
PO Box 85	Orovada	NV	89425-0085	Kings River Ranch Rd. / PO Box 85
PO Box 33	Paradise Valley	NV	89426-0013	275 Bridge St / PO Box 33
5495 Palisade Drive	Winnemucca	NV	89445-4156	5495 Palisade Drive
1500 Melarkey Street	Winnemucca	NV	89445-3830	1500 Melarkey Street
PO Box 98	McDermitt	NV	89421-0098	100 Olavarria Street
6465 South Grass Valley Road	Winnemucca	NV	89445-7258	6465 South Grass Valley Road
451 Reinhart Street	Winnemucca	NV	89445-3055	451 Reinhart Street

PO Box 98	McDermitt	NV	89421-0098	100 Olavarria Street
5375 Kluncy Canyon Road	Winnemucca	NV	89445-3964	5375 Kluncy Canyon Road
PO Box 98	McDermitt	NV	89421-0098	100 Olavarria Street
310 East 4th Street	Winnemucca	NV	89445	310 East 4th Street
310 East 4th Street	Winnemucca	NV	89445	310 East 4th Street
PO Box 1390	Battle Mountain	NV	89820	650 Altenburg Avenue
PO Box 1360	Battle Mountain	NV	89820	985 W. Humboldt
PO Box 1330	Battle Mountain	NV	89820	425 Weaver Ave
PO Box 160	Austin	NV	89310	200 Highway 305 North Box 160
PO Box 1300	Battle Mountain	NV	89820	625 Weaver Ave
P.O. Box 170	Alamo	NV	89001	593 Broadway
P.O. Box 767	Caliente	NV	89008	289 Lincoln Street
P.O. Box 307	Panaca	NV	89042	1000 East Edwards
P.O. Box 30	Pioche	NV	89043	651 Airport Road
P.O. Box 567	Panaca	NV	89042	91 N 4th Street
P.O. Box 298	Alamo	NV	89001	158 Main Street
P.O. Box 268	Panaca	NV	89042	1111 East Edwards Street
P.O. Box 298	Alamo	NV	89001	158 Main Street
P.O. Box 1088	Caliente	NV	89008	500 Youth Center Drive
P.O. Box 118	Panaca	NV	89008	1005 Main ST. Suite 108
P.O. Box 118	Panaca	NV	89042	1005 Main ST. Suite 108
285 Dayton Valley Road	Dayton	NV	89403	285 Dayton Valley Road
112 N. California Street	Yerington	NV	89447	112 N. California Street
450 Hardie Lane	Fernley	NV	89408	450 Hardie Lane
3900 W. Spruce Avenue	Silver Springs	NV	89429	3900 W. Spruce Avenue
4180 Farm District Road	Fernley	NV	89408	4180 Farm District Road
315 Dayton Valley Road	Dayton	NV	89403	315 Dayton Valley Road
925 Farm District Road	Fernley	NV	89408	925 Farm District Road
190 Dayton Village Parkway	Dayton	NV	89403	190 Dayton Village Parkway
1200 Ferretto Parkway	Dayton	NV	89403	1200 Ferretto Parkway
215 Pearl Street	Yerington	NV	89447	215 Pearl Street
320 Hwy 95A South	Fernley	NV	89408	320 Hwy 95A South
3800 W. Spruce Avenue	Silver Springs	NV	89429	3800 W. Spruce Avenue
1100 Jasmine Lane	Fernley	NV	89408	1100 Jasmine Lane
1300 Hwy 95A South	Fernley	NV	89408	1300 Hwy 95A South

20 Day Lane	Smith	NV	89430	20 Day Lane
114 Pearl Street	Yerington	NV	89447	114 Pearl Street
335 Dayton Valley Road	Dayton	NV	89403	335 Dayton Valley Road
3755 W. Spruce Avenue	Silver Springs	NV	89429	3755 W. Spruce Avenue
3755 W. Spruce Street	Silver Springs	NV	89429	3755 W. Spruce Street
1340 Hwy 95A South	Fernley	NV	89408	1340 Hwy 95A South
25 E. Goldfield Avenue	Yerington	NV	89447	25 E. Goldfield Avenue
3655 Spruce Avenue	Silver Springs	NV	89429	3655 Spruce Avenue
Box 1060	Hawthorne	NV	89415	301 W. 9th St
Box 70	Schurz	NV	89427	4048 S. Hwy 95
Box 938	Hawthorne	NV	89415	601 A St
PO Box 938	Hawthorne	NV	89415	601 A St
751 A St	Hawthorne	NV	89415	751 A St
4881 N Lola Ln	Pahrump	NV	89060	4881 N Lola Ln
PO Box 1429	Round Mountain	NV	89045	59 Hadley Cir
PO Box 147	Gabbs	NV	89409	511 East Ave
1560 E. Amargosa Farm Rd.	Amargosa	NV	89020	1560 E. Amargosa Farm Rd.
900 E Jack Rabbit St	Pahrump	NV	89048	900 E Jack Rabbit St
PO Box 369	Beatty	NV	89003	301 N 4th St
PO Box 1749	Tonopah	NV	89049	1220 Idaho Cir
1521 E Idaho St	Pahrump	NV	89048	1521 E Idaho St
7120 S Hafen Ranch Rd	Pahrump	NV	89061	7120 S Hafen Ranch Rd
6181 S. Jane Ave	Pahrump	NV	89061	6181 S Jane Ave
4201 N Blagg Rd	Pahrump	NV	89060	4201 N Blagg Rd
PO Box 369	Beatty	NV	89003	301 N 4th St
PO Box 1749	Tonopah	NV	89049	1220 Idaho Cir
PO Box 1427	Round Mountain	NV	89045	61 Hadley Cir
PO Box 147	Gabbs	NV	89409	511 East Ave
1560 E. Amargosa Farm Rd.	Amargosa	NV	89020	1560 E. Amargosa Farm Rd.
PO Box 806	Beatty	NV	89003	1 Hornet Ave
PO Box 147	Gabbs	NV	89409	511 East Ave
PO Box 1349	Tonopah	NV	89049	1 Ray Tennant Dr
501 E Calvada Blvd	Pahrump	NV	89048	501 E Calvada Blvd
PO Box 1427	Round Mountain	NV	89045	61 Hadley Cir
2765 Mt. Charleston Drive	Pahrump	NV	89048	2765 Mt. Charleston Drive

2765 Mt. Charleston Drive	Pahrump	NV	89048	2765 Mt. Charleston Drive
2765 Mt. Charleston Drive	Pahrump	NV	89048	2765 Mt. Charleston Drive
2765 Mt. Charleston Drive	Pahrump	NV	89048	2765 Mt. Charleston Drive
110 Thompson St.	Carson City	NV	89703	110 S. Thompson St.
275 East Park St. Bldg. E	Carson City	NV	89706	275 East Park St. Bldg. E
504 Bath St.	Carson City	NV	89703	504 Bath St.
1511 Firebox Rd.	Carson City	NV	89701	1511 Firebox Rd.
2800 S. Saliman Rd.	Carson City	NV	89701	2800 S. Saliman Rd.
1260 Monte Rosa Dr.	Carson City	NV	89701	1260 Monte Rosa Dr.
2111 Carriage Crest Dr.	Carson City	NV	89706	2111 Carriage Crest Dr.
2263 Mouton Dr.	Carson City	NV	89706	2263 Mouton Dr.
1140 W. King St.	Carson City	NV	89703	1140 W. King St.
4151 E. Fifth St.	Carson City	NV	89701	4151 E. Fifth St.
1111 N. Saliman Rd.	Carson City	NV	89701	1111 N. Saliman Rd.
PO Box 86	Imlay	NV	89418	380 Main Street
PO Box 621	Lovelock	NV	89419	1100 Harvard Way
PO Box 1020	Lovelock	NV	89419	1295 Elmhurst Avenue
PO Box 990	Lovelock	NV	89419	1215 Franklin Avenue
765 Western Avenue	Lovelock	NV	89419	765 Western Avenue
1200 Prison Road	Lovelock	NV	89419	1200 Prison Road
PO Box C	Virginia City	NV	89440	191 South D Street
1250 Peri Ranch Road	Sparks	NV	89434	1250 Peri Ranch Road
PO Box C	Virginia City	NV	89440	127 South D street
PO Box C	Virginia City	NV	89440	95 South R Street
1055 BERRUM LANE	RENO	NV	89509	1055 BERRUM LANE
600 Apple Street	RENO	NV	89502	600 Apple Street
855 MCDONALD DR	RENO	NV	89503	855 MCDONALD DR
1200 MONTELLO ST	RENO	NV	89512	1200 MONTELLO ST
3075 Heights Drive	RENO	NV	89503	3075 Heights Drive
909 HUNTER LAKE DR	RENO	NV	89509	909 HUNTER LAKE DR
1900 Sharon Way	RENO	NV	89509	1900 Sharon Way
1450 STEWART ST	RENO	NV	89502	1450 STEWART ST
2800 Kings Row	RENO	NV	89503	2800 Kings Row
6575 Archimedes Lane	RENO	NV	89523	6575 Archimedes Lane
915 Lander Street	RENO	NV	89509	915 Lander Street

1200 South Meadows Parkway	RENO	NV	89521	1200 South Meadows Parkway
1601 Grandview Ave	RENO	NV	89503	1601 Grandview Ave
2450 Cannan Street	RENO	NV	89512	2450 Cannan Street
1901 Villanova Drive	RENO	NV	89502	1901 Villanova Drive
4000 MAYBERRY DR	RENO	NV	89519	4000 MAYBERRY DR
4801 Neil Road	RENO	NV	89502	4801 Neil Road
926 Cloudburst St	RENO	NV	89506	926 Cloudburst St
1200 Locust Street	RENO	NV	89502	1200 Locust Street
1900 Sullivan Lane	SPARKS	NV	89431	1900 Sullivan Lane
2300 North Rock Blvd	SPARKS	NV	89431	2300 North Rock Blvd
2755 Fourth Street	SPARKS	NV	89431	2755 Fourth Street
1840 4TH STREET	SPARKS	NV	89431	1840 4TH STREET
1925 F STREET	SPARKS	NV	89431	1925 F STREET
225 QUEEN WAY	SPARKS	NV	89431	225 QUEEN WAY
201 Lincoln Way	SPARKS	NV	89431	201 Lincoln Way
1216 Prater Way	SPARKS	NV	89431	1216 Prater Way
13815 Spelling Court	RENO	NV	89521	13815 Spelling Court
980 WHEATLAND RD	RENO	NV	89511	980 WHEATLAND RD
2001 SOARING EAGLE DR	RENO	NV	89512	2001 SOARING EAGLE DR
255 W Patrician Drive	RENO	NV	89506	255 W Patrician Drive
405 SURREY DRIVE	RENO	NV	89511	405 SURREY DRIVE
5490 LEON DRIVE	SPARKS	NV	89433	5490 LEON DRIVE
PO BOX 309	VERDI	NV	89439	250 Bridge Street
PO Box 130	WADSWORTH	NV	89442	1 Hwy 447
1735 DEL ROSA WAY	SPARKS	NV	89434	1735 DEL ROSA WAY
1135 O CALLAGHAN DR	SPARKS	NV	89434	1135 O CALLAGHAN DR
5890 KLONDIKE	SPARKS	NV	89433	5890 KLONDIKE
185 SHELBY DRIVE	SPARKS	NV	89436	185 SHELBY DRIVE
5075 ION DRIVE	SPARKS	NV	89436	5075 ION DRIVE
9600 MOJAVE SKY DR	RENO	NV	89521	9600 MOJAVE SKY DR
1100 WINDMILL FARMS PKWY	SPARKS	NV	89436	1100 WINDMILL FARMS PKWY
18001 Briar Drive	Reno	NV	89508	18001 Briar Drive
10600 Green Pasture Dr	Reno	NV	89521	10600 Green Pasture Dr
915 NORTHWOOD BLVD	INCLINE VILLAGE	NV	89451	915 NORTHWOOD BLVD
3870 LIMKIN STREET	RENO	NV	89508	3870 LIMKIN STREET

2500 HOMELAND DRIVE	RENO	NV	89511	2500 HOMELAND DRIVE
4355 HOUSTON DR	RENO	NV	89502	4355 HOUSTON DR
3570 WATERFALL DR	SPARKS	NV	89434	3570 WATERFALL DR
1070 Beckwourth Drive	RENO	NV	89506	1070 Beckwourth Drive
4885 VILLAGE GREEN PKWY	RENO	NV	89519	4885 VILLAGE GREEN PKWY
2115 Alphabet Drive	RENO	NV	89502	2115 Alphabet Drive
8719 Red Baron Blvd	RENO	NV	89506	8719 Red Baron Blvd
1785 Ambassador Drive	RENO	NV	89523	1785 Ambassador Drive
252 Egyptian Way	SPARKS	NV	89441	252 Egyptian Way
5155 MCGUFFY ROAD	SPARKS	NV	89433	5155 MCGUFFEY ROAD
2200 PRIMIO WAY	SPARKS	NV	89434	2200 PRIMIO WAY
13948 MOUNT BISMARK STREET	RENO	NV	89506	13948 MOUNT BISMARK STREET
100 Marilyn Mae Drive	SPARKS	NV	89441	100 Marilyn Mae Drive
1349 BACKER WY	RENO	NV	89523	1349 BACKER WY
2100 Canyon Parkway	SPARKS	NV	89436	2100 Canyon Parkway
5125 Escuela Way	RENO	NV	89502	5125 Escuela Way
2750 ELEMENTARY DR	RENO	NV	89512	2750 ELEMENTARY DR
2505 Crossbow	RENO	NV	89511	2505 Crossbow
5900 Sidehill Drive	SPARKS	NV	89433	5900 Sidehill Drive
7650 CAMPELLO DRIVE	SPARKS	NV	89436	7650 CAMPELLO DRIVE
210 GENTRY WAY	RENO	NV	89502	210 GENTRY WAY
6155 Neil Rd	Reno	NV	89511	6155 Neil Rd
1595 Sky Mountain Dr	Reno	NV	89503	1595 Sky Mountain Dr
3875 GLEN DR	RENO	NV	89502	3875 GLEN STREET
101 FANTASTIC DR	RENO	NV	89512	101 FANTASTIC DR
1295 Wyoming Avenue	RENO	NV	89503	1295 Wyoming Avenue
901 Keele Drive	RENO	NV	89509	901 Keele Drive
1200 Bresson Avenue	RENO	NV	89502	1200 Bresson Avenue
1700 Carville Drive	RENO	NV	89512	1700 Carville Drive
255 PRATER WAY	SPARKS	NV	89431	255 PRATER WAY
2275 18th Street	SPARKS	NV	89431	2275 18th Street
5000 Silver Lake Rd	RENO	NV	89506	5000 Silver Lake Rd
931 SOUTHWOOD BLVD	INCLINE VILLAGE	NV	89451	931 SOUTHWOOD BLVD
6685 CHESTERFIELD LANE	RENO	NV	89523	6685 CHESTERFIELD LANE
1900 Whitewood Drive	SPARKS	NV	89434	1900 Whitewood Drive

6275 NEIL RD	RENO	NV	89511	6275 NEIL RD
9300 WILBUR MAY PARKWAY	RENO	NV	89521	9300 WILBUR MAY PARKWAY
600 EAGLE CANYON DR	SPARKS	NV	89441	600 EAGLE CANYON DR
18235 CODY COURT	RENO	NV	89508	18235 CODY COURT
1701 VALLEY ROAD	RENO	NV	89512	1701 VALLEY ROAD
1200 WINDMILL FARMS	SPARKS	NV	89436	1200 WINDMILL FARMS
1350 E. NINTH ST	RENO	NV	89512	1350 E. NINTH ST
7550 DONATELLO DR	SUN VALLEY	NV	89433	7550 DONATELLO DR
13455 THOMAS CREEK RD	RENO	NV	89511	13455 THOMAS CREEK RD
1331 East Plumb Lane	RENO	NV	89502	1331 East Plumb Lane
395 BOOTH STREET	RENO	NV	89509	395 BOOTH STREET
820 15TH ST	SPARKS	NV	89431	820 15TH ST
3530 Sullivan Lane	Sparks	NV	89431	3530 Sullivan Lane
1350 Baring Blvd.	SPARKS	NV	89434	1350 Baring Blvd.
1155 CORPORATE BLVD	RENO	NV	89502	1155 CORPORATE BLVD
6055 Lancer Street	RENO	NV	89523	6055 Lancer Street
3600 Butch Cassidy Way	RENO	NV	89511	3600 Butch Cassidy Way
777 West Second Street	Reno	NV	89503	777 West Second Street
2880 Sutro Street	Reno	NV	89512	2880 Sutro Street
555 E. Sunset Blvd	GERLACH	NV	89412	555 E. Sunset Blvd
499 VILLAGE BLVD	INCLINE VILLAGE	NV	89451	499 VILLAGE BLVD
7000 DANDINI BLVD	RENO	NV	89512	7000 DANDINI BLVD
5600 Fox Ave	RENO	NV	89506	5600 Fox Ave
1065 EAGLE CANYON DRIVE	SPARKS	NV	89441	1065 EAGLE CANYON DRIVE
1470 EAST GOLDEN VALLEY ROAD	RENO	NV	89506	1470 EAST GOLDEN VALLEY ROAD
2800 VASSAR ST	RENO	NV	89502	2800 VASSAR ST
10500 RIO WRANGLER PKWY	RENO	NV	89521	10500 RIO WRANGLER PKWY
1300 FOSTER DR	RENO	NV	89509	1300 FOSTER DR
380 EDISON WAY	RENO	NV	89502	380 EDISON WAY
240 S Rock BLVD STE 143	Reno	NV	89502	240 S Rock BLVD STE 143
18235 CODY COURT	RENO	NV	89508	18235 CODY COURT
900 FOOTHILL ROAD	RENO	NV	89511	900 FOOTHILL ROAD
350 Hunter Lake Dr	Reno	NV	89509	350 Hunter Lake Dr
2880 SUTRO STREET BLDG B	RENO	NV	89512	2880 SUTRO STREET BLDG B
2880 Sutro Street	RENO	NV	89512	2880 Sutro Street

5450 RIGGINS COURT STE. #6	RENO	NV	89502	5450 RIGGINS COURT STE. #6
240 S Rock Blvd Ste 101	Reno	NV	89502	240 S Rock Blvd Ste 101
PO Box 129	Lund	NV	89317	301 E 2nd North
PO Box 120	Baker	NV	89311	120 Main Street
1001 E 11th ST	Ely	NV	89301	1001 E 11th ST
25 Avenue F	McGill	NV	89318	25 Avenue F
1135 Avenue C	Ely	NV	89301	1800 Bobcat Drive
844 Aultman Street	Ely	NV	89301	844 Aultman Street
1800 Bobcat Drive	Ely	NV	89301	1800 Bobcat Drive
PO Box 129	Lund	NV	89317	301 E 2nd North
700 Aultman Street	Ely	NV	89301	700 Aultman Street
700 Aultman Street	Ely	NV	89301	700 Aultman Street
1135 Avenue C	Ely	NV	89301	1135 Avenue C
1135 Avenue C	Ely	NV	89301	1135 Avenue C
777 E. Ann Rd	North Las Vegas	NV	89081	777 E. Ann Rd
5024 Valley Drive	North Las Vegas	NV	89031	5024 Valley Drive
325 Inflection Street	Henderson	NV	89011	325 Inflection Street
7077 W. Wigwam Avenue	Las Vegas	NV	89113	7077 W. Wigwam Avenue
920 N. Lamb Blvd	Las Vegas	NV	89110	920 N. Lamb Blvd
2680 E. Ninth Street	Reno	NV	89512	2680 E. Ninth Street
2080 East Flamingo Road, Suite 210	Las Vegas	NV	89119	2080 East Flamingo Road, Suite 210
2080 East Flamingo Road, Suite 210	Las Vegas	NV	89119	2080 East Flamingo Road, Suite 210
2080 East Flamingo Road, Suite 210	Las Vegas	NV	89119	2080 East Flamingo Road, Suite 210
2080 East Flamingo Road, Suite 210	Las Vegas	NV	89119	2080 East Flamingo Road, Suite 210
2080 East Flamingo Road, Suite 210	Las Vegas	NV	89119	2080 East Flamingo Road, Suite 210
2080 East Flamingo Road, Suite 210	Las Vegas	NV	89119	2080 East Flamingo Road, Suite 210
2080 East Flamingo Road, Suite 210	Las Vegas	NV	89119	2080 East Flamingo Road, Suite 210
2080 East Flamingo Road, Suite 210	Las Vegas	NV	89119	2080 East Flamingo Road, Suite 210
2080 East Flamingo Road, Suite 210	Las Vegas	NV	89119	2080 East Flamingo Road, Suite 210
2080 East Flamingo Road, Suite 210	Las Vegas	NV	89119	2080 East Flamingo Road, Suite 210
2080 East Flamingo Road, Suite 210	Las Vegas	NV	89119	2080 East Flamingo Road, Suite 210
2080 East Flamingo Road, Suite 210	Las Vegas	NV	89119	2080 East Flamingo Road, Suite 210
2080 East Flamingo Road, Suite 210	Las Vegas	NV	89119	2080 East Flamingo Road, Suite 210
1201 W Lake Mead Blvd	Las Vegas	NV	89106	1201 W Lake Mead Blvd
1095 Fielders Street	Henderson	NV	89011	1095 Fielders Street

4131 E. Bonanza Road	Las Vegas	NV	89110	4131 E. Bonanza Road
3115 Las Vegas Blvd N	Las Vegas	NV	89115	3115 Las Vegas Blvd N
2025 E. Sahara Ave.	Las Vegas	NV	89104	2025 E. Sahara Ave.
3445 Mountain Vista Street	Las Vegas	NV	89121	3445 Mountain Vista Street
4760 East Bonanza Road	Las Vegas	NV	89110	4760 East Bonanza Road
3900 E. Bonanza Rd.	Las Vegas	NV	89110	3900 E. Bonanza Rd.
8377 W Patrick Lane	Las Vegas	NV	89113	8377 W Patrick Lane
7077 W Patrick Lane	Las Vegas	NV	89118	7077 W Patrick Lane
5730 W. Alexander Road	Las Vegas	NV	89130	5730 W. Alexander Road
7495 West Azure Drive, Suite #120	Las Vegas	NV	89130	7495 West Azure Drive, Suite #120
1400 E 13th Street	Ely	NV	89301	1400 E 13th Street
9025 West Cactus Avenue	Las Vegas	NV	89178	9025 West Cactus Avenue
2568 Fire Mesa Street	Las Vegas	NV	89128	2568 Fire Mesa Street
610 Crossbridge Dr.	Las Vegas	NV	89138	610 Crossbridge Dr.
9625 West Saddle Ave	Las Vegas	NV	89147	9625 West Saddle Ave
6435 W. Pebble	Las Vegas	NV	89139	6435 W. Pebble
195 N. Arlington Avenue	Reno	NV	89501	195 N. Arlington Avenue
1360 S Boulder Hwy	Henderson	NV	89015	1360 S Boulder Hwy
225 Grand Cadence Dr.	Henderson	NV	89015	225 Grand Cadence Dr.
2840 Via Contessa	Henderson	NV	89044	2840 Via Contessa
1385 E. Cactus Ave.	Las Vegas	NV	89183	1385 E. Cactus Ave.
675 E. Dale Ave.	Henderson	NV	89044	675 E. Dale Ave.
220 Taylor Street	Henderson	NV	89015	220 Taylor Street
6151 W. Charleston Blvd	Las Vegas	NV	89146	6151 W. Charleston Blvd
385 W. Centennial Parkway	North Las Vegas	NV	89084	385 W. Centennial Parkway
4650 Losee Road	North Las Vegas	NV	89081	4650 Losee Road
4491 N. Rainbow Blvd.	Las Vegas	NV	89108	4491 N. Rainbow Blvd.
7058 Sky Pointe Drive	Las Vegas	NV	89131	7058 Sky Pointe Drive
50 N Stephanie Street	Henderson	NV	89074	50 N Stephanie Street
6475 Valley Drive	North Las Vegas	NV	89084	6475 Valley Drive
8151 N. Shaumber Road	Las Vegas	NV	89166	8151 N. Shaumber Road
5871 Mountain Vista St.	Las Vegas	NV	89120	5871 Mountain Vista St.
4801 S Sandhill Rd	Las Vegas	NV	89121	4801 S Sandhill Rd
8941 Hillpointe Road	Las Vegas	NV	89134	8941 Hillpointe Road
5355 MADRE MESA DR	LAS VEGAS	NV	89108-3541	5355 MADRE MESA DR

950 W Lake Mead Blvd	Las Vegas	NV	89106	950 W Lake Mead Blvd
920 West Williams Avenue, Ste 100	Fallon	NV	89406	920 West Williams Avenue, Ste 100
3725 Butch Cassidy Dr.	Reno	NV	89511	3725 Butch Cassidy Dr.
818 West Brooks Avenue	North Las Vegas	NV	89030	818 West Brooks Avenue
905 W Main Street	Elko	NV	89801	905 W Main Street
1600 E Oakey Blvd	Las Vegas	NV	89104	1600 E Oakey Blvd
950 E. Sahara Ave.	Las Vegas	NV	89104	950 E. Sahara Ave.
4025 N. Rancho Dr.	Las Vegas	NV	89130	4025 N. Rancho Dr.
6610 Grand Montecito Parkway	Las Vegas	NV	89149	6610 Grand Montecito Pkwy
2341 Comstock Dr	North Las Vegas	NV	89032	2341 Comstock Dr
1421 Pullman Dr	Sparks	NV	89434	1421 Pullman Dr
2251 S. Jones Blvd	Las Vegas	NV	89146	2251 S. Jones Blvd
1841 Whitney Mesa Drive	Henderson	NV	89014	1841 Whitney Mesa Drive
100 Youth Center Road	Elko	NV	89801	100 Youth Center Rd
300 N 13th St, 2nd Floor	Las Vegas	NV	89101	300 N 13th St, 2nd Floor
6250 W Charleston Blvd, Ste 150	Las Vegas	NV	89146	6250 W Charleston Blvd Ste 150
233 N Stephanie St	Henderson	NV	89074	233 N. Stephanie St.
2425 North Lamb Boulevard, Suite 130	Las Vegas	NV	89115	2425 North Lamb Boulevard, Suite 130
7885 West Sunset Road, Suite 170	Las Vegas	NV	89113	7885 West Sunset Road, Suite 170
303 S. Water St., Ste 120	Henderson	NV	89015	303 S. Water St., Ste 120
7240 West Azure Dr, Ste 110	Las Vegas	NV	89130	7240 West Azure Dr, Ste 110
4280 West Craig Road, Ste. 102/103	North Las Vegas	NV	89031	4280 West Craig Road, Ste. 102/103
P.O. Box 9119	Reno	NV	89507	1164 N. Virginia St. Jot Travis Building 048
555 Double Eagle Court Suite 1000	Reno	NV	89521	555 Double Eagle Court Suite 1000
8645 S. Eastern Ave. Suite 100	Las Vegas	NV	89123	8645 S. Eastern Ave. Suite 100
7951 Deer Springs	Las Vegas	NV	89131	7951 Deer Springs Way
107 Stafford Dr.	Las Vegas	NV	89115	107 Stafford Dr
1051 Sandy Ridge Ave	Henderson	NV	89052	1051 Sandy Ridge Ave
8185 Tamarus St	Las Vegas	NV	89123	8185 Tamarus St
2150 Windmill Pkwy	Henderson	NV	89074	2150 Windmill Pkwy
7777 Eastgate Rd	Henderson	NV	89011	7777 Eastgate Rd
10 Cadence Crest Ave	Henderson	NV	89011	10 Cadence Crest Ave
7360 W. Flamingo Road	Las Vegas	NV	89147	7360 W. Flamingo Road
3634 Maryland Parkway, Suite 300	Las Vegas	NV	89169	3634 Maryland Parkway, Suite 300
1580 Bledsoe Lane	Las Vegas	NV	89110	1580 Bledsoe Lane

3802 Meadows Ln	Las Vegas	NV	89107	3802 Meadows Ln
4660 N. Rancho Dr.	Las Vegas	NV	89130	4660 N. Rancho Dr.
1031 Railroad Street, Suite 107	Elko	NV	89801	1031 Railroad Street, Suite 107
2101 E Owens Ave.	North Las Vegas	NV	89030	2101 E Owens Ave.
7530 Longley Lane, Suite 103	Reno	NV	89511	7530 Longley Lane, Suite 103
498 S Boulder Hwy	Henderson	NV	89015	498 S Boulder Hwy
1150 Silent Sparrow Drive	Sparks	NV	89441	1150 Silent Sparrow Drive
3551 N Ferrell St	North Las Vegas	NV	89032	3551 N Ferrell St
1501 E Carey Ave.	North Las Vegas	NV	89030	1501 E Carey Ave.
3415 S Mojave Rd	Las Vegas	NV	89121	3415 S Mojave Rd
310 S 9th St	Las Vegas	NV	89101	310 S 9th St
1780 Betty Lane	Las Vegas	NV	89156	1780 Betty Lane
55 N. Valle Verde Dr.	Henderson	NV	89074	55 N. Valle Verde Dr.

Physical City	Physical State	Physical Zip	Phone	Fax
Fallon	NV	89406	(775)423-3463	(775)423-1240
Fallon	NV	89406	(775)423-3159	(775)423-0407
Fallon	NV	89406	(775)423-1999	(775)423-8774
Fallon	NV	89406	(775)428-1996	(775)428-1699
Fallon	NV	89406	(775)423-7701	(775)423-8010
Fallon	NV	89406	(775)423-2181	(775)423-6740
Fallon	NV	89406	(775)423-1191	(775)423-1102
Las Vegas	NV	89178	(702)799-2510	(702)799-2599
Las Vegas	NV	89147	(702)799-2570	(702)799-2585
Las Vegas	NV	89142	(702)799-3200	(702)799-2188
Henderson	NV	89044	(702)799-5888	(702)799-5801
Las Vegas	NV	89141	(702)799-2680	(702)799-2682
Las Vegas	NV	89183	(702)799-5915	(702)799-5929
Las Vegas	NV	89149	(702)799-4585	(702)799-4533
Las Vegas	NV	89179	(702)799-1252	
Las Vegas	NV	89138	(702)799-1420	
Las Vegas	NV	89148	(702)799-2525	
Henderson	NV	89011	(702)799-0220	
Las Vegas	NV	89139	(702)799-8170	
Las Vegas	NV	89110	(702)799-4920	
Las Vegas	NV	89148	(702)799-1360	(702)799-1370
Las Vegas	NV	89149	(702)799-4640	(702)799-4644
N Las Vegas	NV	89084	(702)799-7100	(702)799-7094
Henderson	NV	89044	(702)799-5776	(702)799-5752
Las Vegas	NV	89141	(702)799-2274	(702)799-2295
Las Vegas	NV	89110	(702)799-2140	(702)799-2145
Las Vegas	NV	89139	(702)799-6882	(702)799-6889
Las Vegas	NV	89149	(702)799-6608	(702)799-6618
N Las Vegas	NV	89084	(702)799-1890	(702)799-1865
Las Vegas	NV	89143	(702)799-6600	(702)799-6612
Las Vegas	NV	89178	(702)799-5702	(702)799-5722
Las Vegas	NV	89110	(702)799-2120	(702)799-2143
N Las Vegas	NV	89081	(702)799-1766	(702)799-1769
Las Vegas	NV	89120	(702)799-7500	(702)799-2007

Las Vegas	NV	89106	(702)799-3120	(702)799-1858
Henderson	NV	89002	(702)799-8090	(702)799-8094
N Las Vegas	NV	89032	(702)799-1805	(702)799-1814
N Las Vegas	NV	89081	(702)799-3878	(702)799-3871
Las Vegas	NV	89122	(702)799-7510	(702)799-7515
Las Vegas	NV	89146	(702)799-5890	(702)799-5899
Las Vegas	NV	89178	(702)799-6840	(702)799-6844
Las Vegas	NV	89113	(702)799-2201	(702)799-2204
Las Vegas	NV	89183	(702)799-1380	(702)799-1377
Las Vegas	NV	89183	(702)799-4501	(702)799-4503
Blue Diamond	NV	89004	(702)875-4226	(702)875-4053
Mt Charleston	NV	89124	(702)872-5438	(702)872-0510
Searchlight	NV	89046	(702)297-1224	(702)297-1767
Las Vegas	NV	89156	(702)799-7390	(702)799-7299
Las Vegas	NV	89129	(702)799-4600	(702)799-4609
Las Vegas	NV	89147	(702)799-5990	(702)799-5979
Las Vegas	NV	89123	(702)799-5700	(702)799-5711
Las Vegas	NV	89117	(702)799-4390	(702)799-1413
Las Vegas	NV	89130	(702)799-4530	(702)799-4540
Henderson	NV	89002	(702)799-8060	(702)799-8076
Las Vegas	NV	89142	(702)799-8680	(702)799-7464
Las Vegas	NV	89128	(702)799-4350	(702)799-4307
Moapa	NV	89025	(702)864-2444	(702)864-2566
Las Vegas	NV	89115	(702)799-8820	(702)799-8895
Las Vegas	NV	89115	(702)799-4970	(702)855-9245
Las Vegas	NV	89101	(702)799-8360	(702)799-8372
Las Vegas	NV	89129	(702)799-4680	(702)799-4677
Las Vegas	NV	89108	(702)799-4890	(702)799-0694
Henderson	NV	89074	(702)799-8730	(702)799-0791
Las Vegas	NV	89146	(702)799-8160	(702)799-8146
Las Vegas	NV	89123	(702)799-5720	(702)799-5719
Las Vegas	NV	89145	(702)799-4320	(702)799-4359
Las Vegas	NV	89117	(702)799-4370	(702)799-4341
Las Vegas	NV	89122	(702)799-8780	(702)799-0881
Henderson	NV	89074	(702)799-5730	(702)799-5759

Henderson	NV	89014	(702)799-8760	(702)799-0916
Las Vegas	NV	89110	(702)799-7380	(702)799-7327
Las Vegas	NV	89156	(702)799-8860	(702)799-8884
Las Vegas	NV	89119	(702)799-5690	(702)799-5698
Las Vegas	NV	89110	(702)799-8800	(702)799-2115
Las Vegas	NV	89130	(702)799-4690	(702)799-4544
Las Vegas	NV	89129	(702)799-4660	(702)799-4666
Las Vegas	NV	89128	(702)799-4330	(702)799-4306
Las Vegas	NV	89118	(702)799-8140	(702)799-8198
Boulder City	NV	89005	(702)799-8260	(702)799-8269
Henderson	NV	89074	(702)799-5750	(702)799-5739
Las Vegas	NV	89147	(702)799-4440	(702)799-4319
Henderson	NV	89014	(702)799-0740	(702)799-0775
N Las Vegas	NV	89031	(702)799-8380	(702)799-8355
Las Vegas	NV	89134	(702)799-4380	(702)799-4310
Las Vegas	NV	89123	(702)799-5760	(702)799-5770
N Las Vegas	NV	89030	(702)799-0600	(702)799-7045
Las Vegas	NV	89115	(702)799-4930	(702)799-4927
Las Vegas	NV	89117	(702)799-4450	(702)799-1410
Henderson	NV	89015	(702)799-0500	(702)799-0511
N Las Vegas	NV	89032	(702)799-0620	(702)799-0610
Las Vegas	NV	89128	(702)799-1460	(702)799-1469
N Las Vegas	NV	89032	(702)799-1750	(702)799-1756
Henderson	NV	89074	(702)799-1320	(702)799-1326
Las Vegas	NV	89149	(702)799-4580	(702)799-4586
N Las Vegas	NV	89031	(702)799-1860	(702)799-1869
Las Vegas	NV	89142	(702)799-1550	(702)799-1556
Henderson	NV	89012	(702)799-0540	(702)799-0546
Las Vegas	NV	89101	(702)799-1700	(702)799-1706
Las Vegas	NV	89147	(702)799-1270	(702)799-1276
Las Vegas	NV	89144	(702)799-6050	(702)799-6056
Las Vegas	NV	89123	(702)799-1350	(702)799-1356
Bunkerville	NV	89007	(702)346-1900	(702)346-1914
Las Vegas	NV	89131	(702)799-3450	(702)799-3456
N Las Vegas	NV	89031	(702)799-3150	(702)799-3156

Henderson	NV	89015	(702)799-3550	(702)799-3556
Las Vegas	NV	89108	(702)799-3420	(702)799-3476
N Las Vegas	NV	89031	(702)799-1730	(702)799-1722
Las Vegas	NV	89115	(702)799-2180	(702)799-3219
Henderson	NV	89052	(702)799-1330	(702)799-1347
Las Vegas	NV	89129	(702)799-6000	(702)799-6012
Las Vegas	NV	89147	(702)799-6030	(702)799-4466
Henderson	NV	89074	(702)799-6300	(702)799-6306
Las Vegas	NV	89130	(702)799-2200	(702)799-4576
Las Vegas	NV	89130	(702)799-6650	(702)799-6659
Las Vegas	NV	89149	(702)799-6630	(702)799-6651
Las Vegas	NV	89131	(702)799-6690	(702)799-6674
Las Vegas	NV	89148	(702)799-6870	(702)799-2222
Las Vegas	NV	89104	(702)799-3750	(702)799-3723
Henderson	NV	89012	(702)799-6860	(702)799-6864
N Las Vegas	NV	89031	(702)799-7040	(702)799-7028
Las Vegas	NV	89139	(702)799-2590	(702)799-2622
Las Vegas	NV	89110	(702)799-7250	(702)799-7241
N Las Vegas	NV	89031	(702)799-0690	(702)799-0665
Las Vegas	NV	89123	(702)799-6899	(702)799-6891
Las Vegas	NV	89142	(702)799-7260	(702)799-7329
Henderson	NV	89002	(702)799-0570	(702)799-0537
Las Vegas	NV	89129	(702)799-1402	(702)799-1414
Las Vegas	NV	89138	(702)799-1430	(702)799-1485
Las Vegas	NV	89135	(702)799-2520	(702)799-1233
Las Vegas	NV	89183	(702)799-6810	(702)799-6803
Las Vegas	NV	89143	(702)799-3401	(702)799-3433
N Las Vegas	NV	89031	(702)799-1891	(702)799-1812
Las Vegas	NV	89148	(702)799-2504	(702)799-1289
N Las Vegas	NV	89081	(702)799-4701	(702)799-4707
Las Vegas	NV	89103	(702)799-2550	(702)799-2545
Las Vegas	NV	89148	(702)799-1920	(702)799-1912
Las Vegas	NV	89141	(702)799-1240	(702)799-1275
Las Vegas	NV	89156	(702)799-1899	(702)799-1612
Las Vegas	NV	89115	(702)799-2100	(702)799-2110

N Las Vegas	NV	89084	(702)799-1770	(702)799-1721
Las Vegas	NV	89149	(702)799-3430	(702)799-3432
N Las Vegas	NV	89084	(702)799-3870	(702)799-3877
Las Vegas	NV	89178	(702)799-5701	(702)799-5708
Las Vegas	NV	89108	(702)799-4780	(702)799-4788
Las Vegas	NV	89106	(702)799-4740	(702)799-4884
Las Vegas	NV	89101	(702)799-7159	(702)799-7164
N Las Vegas	NV	89030	(702)799-7169	(702)799-7109
Las Vegas	NV	89104	(702)799-7890	(702)799-7884
N Las Vegas	NV	89032	(702)799-4730	(702)799-4728
Las Vegas	NV	89146	(702)799-4205	(702)799-4183
Las Vegas	NV	89107	(702)799-4200	(702)799-0319
N Las Vegas	NV	89030	(702)799-7123	(702)799-8337
Las Vegas	NV	89101	(702)799-7896	(702)799-8526
Las Vegas	NV	89106	(702)799-4720	(702)799-4727
Las Vegas	NV	89110	(702)799-7310	(702)799-8817
Las Vegas	NV	89115	(702)799-4900	(702)799-4904
Las Vegas	NV	89121	(702)799-7780	(702)799-0719
Las Vegas	NV	89121	(702)799-7401	(702)799-0118
Las Vegas	NV	89104	(702)799-7904	(702)799-7949
N Las Vegas	NV	89030	(702)799-7139	(702)799-7132
Las Vegas	NV	89108	(702)799-4770	(702)799-3170
Las Vegas	NV	89106	(702)799-7113	(702)799-0401
Las Vegas	NV	89121	(702)799-7710	(702)799-8798
Las Vegas	NV	89119	(702)799-5540	(702)799-0299
N Las Vegas	NV	89030	(702)799-7133	(702)799-1724
N Las Vegas	NV	89030	(702)799-4910	(702)799-4942
Las Vegas	NV	89106	(702)799-4760	(702)799-4765
N Las Vegas	NV	89030	(702)799-7103	(702)799-0406
Las Vegas	NV	89106	(702)799-4750	(702)799-0699
Las Vegas	NV	89121	(702)799-8692	(702)999-9999
Las Vegas	NV	89156	(702)799-7350	(702)799-7398
Henderson	NV	89052	(702)799-6892	(702)799-2276
Las Vegas	NV	89107	(702)799-4185	(702)799-4172
Las Vegas	NV	89119	(702)799-5660	(702)895-2038

Las Vegas	NV	89108	(702)799-4800	(702)799-0611
N Las Vegas	NV	89030	(702)799-7149	(702)799-7043
Las Vegas	NV	89107	(702)799-4223	(702)799-4164
Las Vegas	NV	89102	(702)799-5910	(702)799-5916
Las Vegas	NV	89169	(702)799-5530	(702)799-0270
Las Vegas	NV	89107	(702)799-4233	(702)799-0317
Las Vegas	NV	89169	(702)799-5550	(702)799-1160
Las Vegas	NV	89101	(702)799-7912	(702)799-8556
N Las Vegas	NV	89030	(702)799-7179	(702)799-8341
Las Vegas	NV	89108	(702)799-4790	(702)799-4899
Las Vegas	NV	89107	(702)799-4213	(702)799-0315
Las Vegas	NV	89102	(702)799-5960	(702)799-5975
Las Vegas	NV	89101	(702)799-7095	(702)799-7102
Las Vegas	NV	89107	(702)799-4239	(702)799-4252
Las Vegas	NV	89121	(702)799-7700	(702)799-0792
Henderson	NV	89015	(702)799-8930	(702)799-8910
Boulder City	NV	89005	(702)799-8280	(702)799-8272
Henderson	NV	89015	(702)799-8940	(702)799-8965
Indian Springs	NV	89018	(702)799-0932	(702)879-3142
N Las Vegas	NV	89032	(702)799-6200	(702)799-4787
Henderson	NV	89015	(702)799-8950	(702)799-8984
Mesquite	NV	89027	(702)346-5761	(702)346-5049
Las Vegas	NV	89122	(702)799-7790	(702)799-0933
Las Vegas	NV	89121	(702)799-7720	(702)799-0798
Las Vegas	NV	89119	(702)799-5650	(702)799-5658
Las Vegas	NV	89142	(702)799-8600	(702)799-0116
Las Vegas	NV	89115	(702)799-7360	(702)799-7287
Las Vegas	NV	89120	(702)799-7740	(702)799-7748
Las Vegas	NV	89121	(702)799-7750	(702)799-0785
Las Vegas	NV	89147	(702)799-5930	(702)799-5925
Las Vegas	NV	89145	(702)799-4300	(702)799-4436
Las Vegas	NV	89120	(702)799-7770	(702)799-0726
Las Vegas	NV	89103	(702)799-5940	(702)799-1210
Las Vegas	NV	89110	(702)799-7320	(702)799-8890
Las Vegas	NV	89120	(702)799-7730	(702)799-0757

Las Vegas	NV	89103	(702)799-5920	(702)799-5924
Las Vegas	NV	89104	(702)799-7456	(702)799-7460
Las Vegas	NV	89143	(702)799-4646	(702)799-4538
Las Vegas	NV	89141	(702)799-2298	(702)799-6859
Las Vegas	NV	89101	(702)799-1660	(702)799-1666
Las Vegas	NV	89115	(702)799-8830	(702)799-3259
Las Vegas	NV	89110	(702)799-7330	(702)799-7339
Henderson	NV	89002	(702)799-8920	(702)799-8927
Henderson	NV	89014	(702)799-7760	(702)799-8795
Las Vegas	NV	89146	(702)799-5950	(702)799-5978
Logandale	NV	89021	(702)398-3233	(702)398-3278
Las Vegas	NV	89183	(702)799-2220	(702)799-1372
N Las Vegas	NV	89030	(702)799-3800	(702)799-3804
Las Vegas	NV	89110	(702)799-3270	(702)799-3269
Las Vegas	NV	89135	(702)799-6077	(702)799-6704
Las Vegas	NV	89122	(702)799-3700	(702)799-3711
Las Vegas	NV	89129	(702)799-6710	(702)799-4317
Las Vegas	NV	89144	(702)799-6720	(702)799-6070
Henderson	NV	89052	(702)799-2230	(702)799-2257
Las Vegas	NV	89169	(702)799-1120	(702)799-3397
Las Vegas	NV	89108	(702)799-4500	(702)799-4520
Sandy Valley	NV	89019	(702)723-5344	(702)723-5251
Laughlin	NV	89029	(702)298-3378	(702)299-0405
Las Vegas	NV	89115	(702)799-4990	(702)799-4997
Las Vegas	NV	89110	(702)799-7272	(702)799-7303
Las Vegas	NV	89108	(702)799-4777	(702)799-0680
Las Vegas	NV	89118	(702)799-8181	(702)799-8188
Henderson	NV	89015	(702)799-8990	(702)799-0599
Henderson	NV	89014	(702)799-7788	(702)799-0948
Las Vegas	NV	89106	(702)799-1830	(702)799-3106
Las Vegas	NV	89115	(702)799-7280	(702)799-7286
Las Vegas	NV	89107	(702)799-4245	(702)799-4296
Las Vegas	NV	89107	(702)799-4260	(702)799-0348
Las Vegas	NV	89102	(702)799-5880	(702)799-5947
N Las Vegas	NV	89030	(702)799-7080	(702)799-7195

Las Vegas	NV	89108	(702)799-4550	(702)799-4549
N Las Vegas	NV	89030	(702)799-7185	(702)799-7074
Las Vegas	NV	89104	(702)799-5558	(702)799-5566
Las Vegas	NV	89104	(702)799-7470	(702)799-0157
Las Vegas	NV	89107	(702)799-4700	(702)799-4705
Las Vegas	NV	89101	(702)799-7922	(702)799-7959
Las Vegas	NV	89119	(702)799-5573	(702)799-0297
Henderson	NV	89015	(702)799-8080	(702)799-8088
Las Vegas	NV	89121	(702)799-7660	(702)799-0805
Las Vegas	NV	89120	(702)799-5600	(702)799-5644
Las Vegas	NV	89103	(702)799-5900	(702)799-5905
Boulder City	NV	89005	(702)799-8290	(702)799-8252
Henderson	NV	89015	(702)799-8900	(702)799-3511
Sandy Valley	NV	89019	(702)723-1800	(702)723-1802
Laughlin	NV	89029	(702)298-1996	(702)298-5493
Las Vegas	NV	89110	(702)799-7340	(702)799-8870
Las Vegas	NV	89145	(702)799-4480	(702)799-4497
Henderson	NV	89074	(702)799-0920	(702)799-0925
N Las Vegas	NV	89032	(702)799-4860	(702)799-4806
Henderson	NV	89014	(702)799-0777	(702)799-7690
Las Vegas	NV	89134	(702)799-4460	(702)799-4470
Las Vegas	NV	89118	(702)799-5980	(702)799-5969
Overton	NV	89040	(702)397-8610	(702)397-2754
Las Vegas	NV	89106	(702)799-3120	(702)799-3126
Las Vegas	NV	89130	(702)799-4620	(702)799-4626
Las Vegas	NV	89110	(702)799-3220	(702)799-3226
Las Vegas	NV	89129	(702)799-3400	(702)799-3407
Las Vegas	NV	89123	(702)799-2240	(702)799-2247
Las Vegas	NV	89122	(702)799-2400	(702)799-2407
Indian Springs	NV	89018	(702)799-0932	(702)879-3142
Las Vegas	NV	89147	(702)799-2540	(702)799-2563
Henderson	NV	89052	(702)799-2260	(702)799-1309
Las Vegas	NV	89144	(702)799-6040	(702)799-6094
Las Vegas	NV	89129	(702)799-4699	(702)799-4528
N Las Vegas	NV	89084	(702)799-7020	(702)799-8346

Las Vegas	NV	89115	(702)799-3670	(702)799-3202
Las Vegas	NV	89123	(702)799-2290	(702)799-5717
N Las Vegas	NV	89032	(702)799-3880	(702)799-1785
Las Vegas	NV	89142	(702)799-3240	(702)799-3286
Las Vegas	NV	89148	(702)799-1900	(702)799-5688
Las Vegas	NV	89131	(702)799-6692	(702)799-4536
Las Vegas	NV	89139	(702)799-1340	(702)799-5715
Mesquite	NV	89027	(702)346-3250	(702)346-3095
N Las Vegas	NV	89031	(702)799-3160	(702)799-3169
Henderson	NV	89002	(702)799-3020	(702)799-3501
Las Vegas	NV	89131	(702)799-3460	(702)799-4511
Henderson	NV	89052	(702)799-1305	(702)799-1310
Las Vegas	NV	89121	(702)799-2005	(702)799-2412
Las Vegas	NV	89156	(702)799-4811	(702)799-4807
N Las Vegas	NV	89081	(702)799-7001	(702)799-7010
Las Vegas	NV	89141	(702)799-6801	(702)799-6805
Las Vegas	NV	89149	(702)799-4560	(702)799-4568
Las Vegas	NV	89148	(702)799-6850	(702)799-6852
Las Vegas	NV	89178	(702)799-2560	(702)799-2635
NORTH LAS VEGAS	NV	89030	(702)799-7139	(702)799-7132
Las Vegas	NV	89102	(702)799-5800	(702)799-5813
Las Vegas	NV	89142	(702)799-0180	(702)799-0192
Las Vegas	NV	89101	(702)799-7000	(702)799-8316
Las Vegas	NV	89169	(702)799-5450	(702)799-1074
Las Vegas	NV	89107	(702)799-4080	(702)799-4104
Henderson	NV	89015	(702)799-8000	(702)799-8966
Las Vegas	NV	89110	(702)855-9765	
Las Vegas	NV	89121	(702)799-7580	(702)799-0776
Las Vegas	NV	89110	(702)799-7200	(702)799-7255
Las Vegas	NV	89146	(702)799-4000	(702)799-4078
Las Vegas	NV	89120	(702)799-7500	(702)799-2007
Las Vegas	NV	89128	(702)799-4400	(702)799-4425
N Las Vegas	NV	89032	(702)799-4830	(702)799-4856
Henderson	NV	89014	(702)799-0950	(702)799-0717
Las Vegas	NV	89113	(702)799-5850	(702)799-5855

Las Vegas	NV	89101	(702)799-7800	(702)799-7948
Las Vegas	NV	89106	(702)799-7870	(702)799-0656
Las Vegas	NV	89123	(702)799-5790	(702)799-5744
N Las Vegas	NV	89030	(702)651-4070	(702)651-4627
Las Vegas	NV	89146	(702)651-5030	(702)651-5035
N Las Vegas	NV	89031	(702)799-0432	(702)799-0437
Las Vegas	NV	89144	(702)799-1450	(702)799-1455
Henderson	NV	89002	(702)651-3080	(702)651-3075
Las Vegas	NV	89131	(702)799-6699	(702)799-4698
Henderson	NV	89052	(702)799-2270	(702)799-6858
N Las Vegas	NV	89032	(702)799-1870	(702)799-1876
Las Vegas	NV	89120	(702)799-6830	(702)799-2235
Las Vegas	NV	89147	(702)799-2580	(702)799-1288
Las Vegas	NV	89106	(702)799-4710	(702)799-4722
Las Vegas	NV	89113	(702)799-5766	(702)799-5751
Las Vegas	NV	89156	(702)799-7207	(702)799-7212
Las Vegas	NV	89135	(702)799-4340	(702)799-4355
Henderson	NV	89012	(702)799-2250	(702)799-2225
Boulder City	NV	89005	(702)799-8200	(702)799-8230
Overton	NV	89040	(702)397-2611	(702)397-2892
Mesquite	NV	89027	(702)346-2780	(702)346-7265
Indian Springs	NV	89018	(702)799-0932	(702)879-3142
Las Vegas	NV	89149	(702)799-3440	(702)799-3443
Henderson	NV	89002	(702)799-3500	(702)799-3524
Las Vegas	NV	89110	(702)799-2196	(702)799-2198
Las Vegas	NV	89113	(702)799-6820	(702)799-6847
Henderson	NV	89052	(702)799-6800	(702)799-6839
Las Vegas	NV	89131	(702)799-6660	(702)799-6669
N Las Vegas	NV	89084	(702)799-1777	(702)799-1701
Las Vegas	NV	89149	(702)799-4640	(702)799-4644
Las Vegas	NV	89141	(702)799-6881	(702)799-6888
Las Vegas	NV	89142	(702)799-8888	(702)799-8899
Las Vegas	NV	89121	(702)799-6852	(702)799-0704
Las Vegas	NV	89121	(702)799-6852	
Las Vegas	NV	89104	(702)799-0250	(702)799-0084

North Las Vegas	NV	89084	(702)799-1720	(702)799-1711
North Las Vegas	NV	89032	(702)952-9773	
Las Vegas	NV	89101	(702)799-1623	(702)799-1633
North Las Vegas	NV	89084	(702)799-1720	
Las Vegas	NV	89183	(702)799-1111	(702)855-7309
North Las Vegas	NV	89032	(702)799-4830	
Las Vegas	NV	89128	(702)799-4400	
Las Vegas	NV	89110	(702)799-2196	
Las Vegas	NV	89107	(702)799-4080	
Las Vegas	NV	89146	(702)799-4000	
Las Vegas	NV	89169	(702)799-5588	(702)799-5592
Las Vegas	NV	89101	(702)799-7938	(702)799-7956
Las Vegas	NV	89101	(702)799-1623	(702)799-1633
Las Vegas	NV	89115	(702)455-5555	(702)382-6035
Las Vegas	NV	89101	(702)799-5631	(702)799-5642
Las Vegas	NV	89101	(702)799-5631	(702)799-5642
Las Vegas	NV	89115	(702)799-0275	(702)799-0268
Las Vegas	NV	89103	(702)799-8150	(702)799-1207
Las Vegas	NV	89104	(702)799-8850	(702)799-8898
Las Vegas	NV	89122	(702)799-6370	(702)799-6377
Las Vegas	NV	89101	(702)799-5631	(702)999-9999
Las Vegas	NV	89101	(702)799-5631	(702)999-9999
Las Vegas	NV	89103	(702)799-2070	(702)799-2089
Las Vegas	NV	89122	(702)799-6380	(702)799-6388
Las Vegas	NV	89149	(702)799-6610	(702)799-6604
Las Vegas	NV	89101	(702)799-7938	(702)799-7956
Las Vegas	NV	89101	(702)799-1623	(702)799-1633
Las Vegas	NV	89101	(702)799-1623	(702)799-1633
Indian Springs	NV	89070	(702)879-6682	(702)879-6626
Las Vegas	NV	89104	(702)799-8650	(702)799-8608
Indian Springs	NV	89070	(702)879-1381	(702)879-1383
N Las Vegas	NV	89115	(702)651-7227	(702)668-7229
N Las Vegas	NV	89030	(702)799-6240	(702)799-6260
Indian Springs	NV	89018	(702)879-6824	(702)879-6821
Las Vegas	NV	89101	(702)799-7880	

Boulder City	NV	89005	(702)855-9765	
Las Vegas	NV	89121	(702)799-7463	(702)799-1511
Las Vegas	NV	89101	(702)799-1623	(702)455-5294
Gardnerville	NV	89410	(775)782-5117	(775)782-2115
Zephyr Cove	NV	89448	(775)588-4574	(775)588-4572
Carson City	NV	89705	(775)267-3267	(775)267-3211
Gardnerville	NV	89460	(775)265-2222	(775)265-1218
Minden	NV	89423	(775)267-3622	(775)267-3846
Minden	NV	89423	(775)782-5510	(775)782-5551
Gardnerville	NV	89410	(775)782-2265	(775)782-7341
Gardnerville	NV	89460	(775)265-6100	(775)265-1653
Minden	NV	89423	(775)782-5136	(775)782-7039
Zephyr Cove	NV	89448	(775)588-2446	(775)588-2443
Gardnerville	NV	89410	(775)265-5433	(775)265-6434
Gardnerville	NV	89410	(775)392-1475	(775)783-0930
Gardnerville	NV	89410	(775)392-1480	
Minden	NV	89423	(775)782-5136	
Gardnerville	NV	89410	(775)392-1475	(775)783-0930
Minden	NV	89423	(775)265-5262x1674	(775)782-3946
Elko	NV	89801	(775)756-5597	
Jackpot	NV	89825	(775)755-2375	(775)755-2291
Montello	NV	89830	(775)776-2481	
Spring Creek	NV	89815	(775)744-4382	
Wells	NV	89835	(775)779-2289	
Spring Creek	NV	89815	(775)753-3667	(775)753-4604
Elko	NV	89801	(775)738-7161	(775)778-9144
Elko	NV	89801-2847	(775)738-7255	(775)738-7251
Elko	NV	89801-3326	(775)738-3731	(775)738-9507
Carlin	NV	89822	(775)754-6317	(775)754-2175
Owyhee	NV	89832	(775)757-3400	(775)757-3663
Wells	NV	89835-0338	(775)752-3837	(775)752-2470
West Wendover	NV	89883-2400	(775)664-3100	(775)664-2343
Elko	NV	89801-4414	(775)738-1844	(775)738-2561
Spring Creek	NV	89815	(775)753-6881	(775)753-1074
Spring Creek	NV	89815	(775)738-4711	(775)753-4154

Elko	NV	89801	(775)738-7236	(775)753-3876
Carlin	NV	89822	(775)754-6317	(775)754-2175
Wells	NV	89835	(775)752-3477	(775)752-3411
Elko	NV	89801-2677	(775)738-3375	(775)738-3860
Spring Creek	NV	89815	(775)777-1688	(775)777-1738
Jackpot	NV	89825	(775)755-2375	(775)755-2291
Owyhee	NV	89832	(775)757-3400	(775)757-3663
West Wendover	NV	89883-2400	(775)664-4406	(775)664-4408
Carlin	NV	89822	(775)754-6317	(775)754-2175
Wells	NV	89835	(775)752-3477	(775)752-3411
Elko	NV	89801-3419	(775)738-7281	(775)735-7227
Owyhee	NV	89832	(775)757-3400	(775)757-3663
Jackpot	NV	89825	(775)755-2375	(775)755-2291
Spring Creek	NV	89815	(775)753-5575	(775)753-5953
West Wendover	NV	89883-2400	(775)664-3940	(775)664-3944
Elko	NV	89801	(775)738-5196	(775)777-7458
Elko	NV	89801	(775)753-2233	(775)753-2257
Elko	NV	89801	(775)738-5196	(775)777-1195
Elko	NV	89801	(775)738-5196	
Carlin	NV	89822	(775)397-5032	
Dyer	NV	89010	(775)572-3250	(775)572-3310
Goldfield	NV	89013	(775)485-3215	(775)485-3511
Dyer	NV	89010	(775)572-3250	(775)485-3511
Crescent Valley	NV	89821	(775)468-0213	(775)468-2005
Eureka	NV	89316	(775)237-5700	(775)237-7026
Eureka	NV	89316	(775)237-5361	(775)237-5113
Denio	NV	89404-0076	(866)447-3567	(775)299-5610
Kings River	NV	89425	(866)447-2983	(775)299-5603
Orovada	NV	89425-0085	(866)442-4615	(775)299-5602
Paradise Valley	NV	89426-0013	(866)440-9357	(775)299-5604
Winnemucca	NV	89445-4156	(775)623-8200	
Winnemucca	NV	89445-3830	(775)623-8165	(775)623-8194
McDermitt	NV	89421-0098	(866)447-3991	(775)299-5613
Winnemucca	NV	89445	(775)623-8150	(775)623-8152
Winnemucca	NV	89445-3055	(775)623-8120	(775)623-8208

McDermitt	NV	89421-0098	(866)447-3991	(775)299-5613
Winnemucca	NV	89445-3964	(775)623-8130	(775)623-8185
McDermitt	NV	89421-0098	(866)447-3991	(775)299-5613
Winnemucca	NV	89445	(775)623-8277	(775)623-8278
Winnemucca	NV	89445	(775)623-8240	
Battle Mountain	NV	89820	(775)635-2889	(775)635-6118
Battle Mountain	NV	89820	(775)635-8114	(775)635-8803
Battle Mountain	NV	89820	(775)635-5436	(775)635-5459
Austin	NV	89310	(775)964-2467	(775)964-1206
Battle Mountain	NV	89820	(775)635-6105	(775)635-6110
Alamo	NV	89001	(775)725-3351	(775)725-3355
Caliente	NV	89008	(775)726-3772	(775)726-3880
Panaca	NV	89042	(775)728-4446	(775)728-4470
Pioche	NV	89043	(775)962-5832	(775)962-5257
Panaca	NV	89042	(775)728-4655	(775)728-4302
Alamo	NV	89001	(775)725-3321	(775)725-3334
Panaca	NV	89042	(775)728-4481	(775)728-4484
Alamo	NV	89001	(775)725-3321	(775)725-3334
Caliente	NV	89008	(775)684-5137	(775)726-3371
Panaca	NV	89042	(775)726-8019	(775)728-4533
Panaca	NV	89042	(775)728-8019	(775)728-4533
Dayton	NV	89403	(775)246-6262	(775)246-6264
Yerington	NV	89447	(775)463-6844	(775)463-6850
Fernley	NV	89408	(775)575-3420	(775)575-3428
Silver Springs	NV	89429	(775)577-5060	(775)577-5053
Fernley	NV	89408	(775)575-3332	(775)575-3342
Dayton	NV	89403	(775)246-6250	(775)246-6253
Fernley	NV	89408	(775)575-3414	(775)575-3417
Dayton	NV	89403	(775)246-6270	(775)246-6276
Dayton	NV	89403	(775)246-6170	(775)246-6299
Yerington	NV	89447	(775)463-6833	(775)463-6840
Fernley	NV	89408	(775)575-3390	(775)575-3394
Silver Springs	NV	89429	(775)577-5050	(775)577-5053
Fernley	NV	89408	(775)575-1575	(775)575-1566
Fernley	NV	89408	(775)575-3400	(775)575-3406

Smith	NV	89430	(775)465-2332	(775)465-2681
Yerington	NV	89447	(775)463-6822	(775)463-6828
Dayton	NV	89403	(775)246-6240	(775)246-6248
Silver Springs	NV	89429	(775)577-5071	(775)577-5079
Silver Springs	NV	89429	(775)577-5082	(775)577-5079
Fernley	NV	89408	(775)575-3409	(775)575-3399
Yerington	NV	89447	(775)463-6800	
Silver Springs	NV	89429	(775)577-5128	
Hawthorne	NV	89415	(775)945-1000	(775)945-1009
Schurz	NV	89427	(775)773-2323	(775)773-2275
Hawthorne	NV	89415	(775)945-3332	(775)945-3371
Hawthorne	NV	89415	(775)945-3332	(775)945-3371
Hawthorne	NV	89415	(775)945-2403x11	(775)945-3709
Pahrump	NV	89060	(775)727-5252	(775)727-1526
Round Mountain	NV	89045	(775)377-2236	(775)377-2354
Gabbs	NV	89409	(775)285-2692	(775)285-2381
Amargosa	NV	89020	(775)372-5324	(775)372-5314
Pahrump	NV	89048	(775)727-6619	(775)727-7885
Beatty	NV	89003	(775)553-2902	(775)553-2646
Tonopah	NV	89049	(775)482-6644	(775)482-5717
Pahrump	NV	89048	(775)727-7892	(775)727-7894
Pahrump	NV	89061	(775)751-4688	(775)751-4686
Pahrump	NV	89061	(775)751-4060	(775)751-4001
Pahrump	NV	89060	(775)727-5546	(775)727-7104
Beatty	NV	89003	(775)553-2902	(775)553-2646
Tonopah	NV	89049	(775)482-3698	(775)482-3935
Round Mountain	NV	89045	(775)377-2690	(775)377-2354
Gabbs	NV	89409	(775)285-2692	(775)285-2381
Amargosa	NV	89020	(775)372-5324	(775)372-5314
Beatty	NV	89003	(775)553-2595	(775)553-2887
Gabbs	NV	89409	(775)285-2692	(775)285-2381
Tonopah	NV	89049	(775)482-3698	(775)482-3935
Pahrump	NV	89048	(775)727-7737	(775)727-2284
Round Mountain	NV	89045	(775)377-2690	(775)377-2354
Pahrump	NV	89048	(775)751-6822	(775)751-6829

Pahrump	NV	89048	(775)751-6822	(775)751-6829
Pahrump	NV	89048	(775)751-6822	(775)751-6829
Pahrump	NV	89048	(775)751-6822	(775)751-6829
Carson City	NV	89703	(775)283-2400	(775)283-2490
Carson City	NV	89706	(775)283-1350	(775)283-1391
Carson City	NV	89703	(775)283-1400	(775)283-1490
Carson City	NV	89701	(775)283-1200	(775)283-1290
Carson City	NV	89701	(775)283-2200	(775)283-2290
Carson City	NV	89701	(775)283-1100	(775)283-1190
Carson City	NV	89706	(775)283-1000	(775)283-1090
Carson City	NV	89706	(775)887-9500	(775)887-9502
Carson City	NV	89703	(775)283-2800	(775)283-2890
Carson City	NV	89701	(775)283-2600	(775)283-2690
Carson City	NV	89701	(775)283-1600	(775)283-1790
Imlay	NV	89418	(775)538-7360	(775)273-1250
Lovelock	NV	89419	(775)273-2176	(775)273-1250
Lovelock	NV	89419	(775)273-1200	(775)273-3191
Lovelock	NV	89419	(775)273-2625	(775)273-2163
Lovelock	NV	89419	(775)273-4994	(775)273-4913
Lovelock	NV	89419	(775)977-5415	
Virginia City	NV	89440	(775)847-0977	(775)847-0983
Sparks	NV	89434	(775)342-0400	(775)342-0785
Virginia City	NV	89440	(775)847-0980	(775)847-0913
Virginia City	NV	89440	(775)847-0992	(775)847-0994
RENO	NV	89509	(775)689-2500	(775)689-2622
RENO	NV	89502	(775)689-2540	(775)689-2542
RENO	NV	89503	(775)746-5850	(775)746-5852
RENO	NV	89512	(775)333-5190	(775)333-5193
RENO	NV	89503	(775)746-5830	(775)746-5899
RENO	NV	89509	(775)333-5040	(775)333-5098
RENO	NV	89509	(775)689-2520	(775)689-2598
RENO	NV	89502	(775)333-5140	(775)333-6053
RENO	NV	89503	(775)746-5820	(775)746-5822
RENO	NV	89523	(775)746-7440	(775)746-7443
RENO	NV	89509	(775)333-5030	(775)333-5032

RENO	NV	89521	(775)850-6212	(775)850-6215
RENO	NV	89503	(775)746-5840	(775)746-5841
RENO	NV	89512	(775)353-5750	(775)353-5752
RENO	NV	89502	(775)333-5180	(775)333-5184
RENO	NV	89519	(775)333-5000	(775)333-5002
RENO	NV	89502	(775)689-2560	(775)689-2507
RENO	NV	89506	(775)677-5480	(775)677-5483
RENO	NV	89502	(775)333-5090	(775)333-5092
SPARKS	NV	89431	(775)353-5760	(775)353-5762
SPARKS	NV	89431	(775)353-5580	(775)353-5763
SPARKS	NV	89431	(775)353-5510	(775)353-5512
SPARKS	NV	89431	(775)353-5530	(775)353-5596
SPARKS	NV	89431	(775)353-5720	(775)353-5927
SPARKS	NV	89431	(775)353-5540	(775)353-5759
SPARKS	NV	89431	(775)353-5570	(775)353-5797
SPARKS	NV	89431	(775)353-5590	(775)353-5739
RENO	NV	89521	(775)851-5600	(775)851-5605
RENO	NV	89511	(775)689-2510	(775)689-2623
RENO	NV	89512	(775)333-5080	(775)333-5008
RENO	NV	89506	(775)677-5460	(775)677-5462
RENO	NV	89511	(775)849-0255	(775)849-2761
SPARKS	NV	89433	(775)674-4420	(775)674-4423
VERDI	NV	89439	(775)345-8100	(775)345-7277
WADSWORTH	NV	89442	(775)351-1902	(775)575-1888
SPARKS	NV	89434	(775)353-5730	(775)353-5719
SPARKS	NV	89434	(775)353-5520	(775)353-5522
SPARKS	NV	89433	(775)674-4400	(775)674-4417
SPARKS	NV	89436	(775)425-7755	(775)425-7756
SPARKS	NV	89436	(775)626-5257	(775)626-5258
RENO	NV	89521	(775)852-6570	
SPARKS	NV	89436	(775)626-0062	
RENO	NV	89508	(775)677-3800	
Reno	NV	89521	(775)851-5444	
INCLINE VILLAGE	NV	89451	(775)832-4250	(775)832-4255
RENO	NV	89508	(775)677-5440	(775)677-5435

RENO	NV	89511	(775)851-5620	(775)851-7080
RENO	NV	89502	(775)689-2530	(775)689-2531
SPARKS	NV	89434	(775)626-5200	(775)626-5202
RENO	NV	89506	(775)677-5410	(775)677-5413
RENO	NV	89519	(775)689-2600	(775)689-2535
RENO	NV	89502	(775)857-3150	(775)857-3153
RENO	NV	89506	(775)677-5400	(775)677-5406
RENO	NV	89523	(775)746-5800	(775)746-5803
SPARKS	NV	89441	(775)425-7700	(775)425-7704
SPARKS	NV	89433	(775)674-4430	(775)674-4433
SPARKS	NV	89434	(775)353-5507	(775)353-5905
RENO	NV	89506	(775)677-5444	(775)677-5448
SPARKS	NV	89441	(775)425-7710	(775)425-7707
RENO	NV	89523	(775)746-5810	(775)746-5813
SPARKS	NV	89436	(775)626-5250	(775)626-5254
RENO	NV	89502	(775)689-2626	(775)689-2628
RENO	NV	89512	(775)353-5950	(775)353-5954
RENO	NV	89511	(775)851-7095	(775)850-6204
SPARKS	NV	89433	(775)674-4444	(775)674-4451
SPARKS	NV	89436	(775)425-7722	(775)425-7725
RENO	NV	89502	(775)323-6767	(775)323-6799
Reno	NV	89511	(775)357-9122	
Reno	NV	89503	(775)418-1115	(775)418-1116
RENO	NV	89502	(775)826-4040	(775)826-4040
RENO	NV	89512	(775)624-2800	(775)624-2801
RENO	NV	89503	(775)746-5860	(775)746-5864
RENO	NV	89509	(775)333-5330	(775)333-5083
RENO	NV	89502	(775)333-5160	(775)333-5118
RENO	NV	89512	(775)333-5130	(775)333-5135
SPARKS	NV	89431	(775)353-5740	(775)353-5584
SPARKS	NV	89431	(775)353-5770	(775)353-5585
RENO	NV	89506	(775)677-5420	(775)677-5423
INCLINE VILLAGE	NV	89451	(775)832-4220	(775)832-4210
RENO	NV	89523	(775)746-5870	(775)746-5875
SPARKS	NV	89434	(775)353-5990	(775)353-5994

RENO	NV	89511	(775)829-4601	(775)829-4612
RENO	NV	89521	(775)852-6700	(775)852-6701
SPARKS	NV	89441	(775)425-7777	(775)425-7779
RENO	NV	89508	(775)677-5433	(775)677-5439
RENO	NV	89512	(775)322-0274	(775)322-1328
SPARKS	NV	89436	(775)626-0060	
RENO	NV	89512	(775)323-2332	(775)323-2366
SUN VALLEY	NV	89433	(775)674-4915	
RENO	NV	89511	(775)851-5629	
RENO	NV	89502	(775)321-3160	(775)333-5108
RENO	NV	89509	(775)333-5050	(775)333-5058
SPARKS	NV	89431	(775)353-5550	(775)353-5514
Sparks	NV	89431	(775)333-5300	(775)333-5312
SPARKS	NV	89434	(775)353-5700	(775)353-5708
RENO	NV	89502	(775)857-3181	(775)857-3182
RENO	NV	89523	(775)746-5880	(775)747-6883
RENO	NV	89511	(775)851-5630	(775)851-5607
Reno	NV	89503	(775)333-5150	
Reno	NV	89512	(775)326-0200	
GERLACH	NV	89412	(775)557-2326	(775)557-2587
INCLINE VILLAGE	NV	89451	(775)832-4260	(775)832-4208
RENO	NV	89512	(775)674-7660	(775)674-7931
RENO	NV	89506	(775)677-4500	(775)677-4441
SPARKS	NV	89441	(775)425-7733	(775)425-7735
RENO	NV	89506	(775)677-5499	(775)677-5497
RENO	NV	89502	(775)324-3900	(775)324-3901
RENO	NV	89521	(775)851-5656	(775)851-5663
RENO	NV	89509	(775)322-5566	(775)322-5509
RENO	NV	89502	(775)327-3920	(775)861-4415
Reno	NV	89502	(775)327-0675	(775)857-3158
RENO	NV	89508	(775)677-5433	
RENO	NV	89511	(775)851-5650	(775)851-5652
Reno	NV	89509	(775)337-7560	
RENO	NV	89512	(775)337-9939	(775)333-5324
RENO	NV	89512	(775)337-9939	(775)333-5324

RENO	NV	89502	(775)353-6900	
Reno	NV	89502	(775)327-0685	
Lund	NV	89317	(775)238-5200	(775)238-0208
Baker	NV	89311	(775)234-7333	(775)234-7157
Ely	NV	89301	(775)289-4846	(775)289-4850
McGill	NV	89318	(775)235-7722	(775)235-7036
Ely	NV	89301	(775)289-4811x5103	(775)289-3999
Ely	NV	89301	(775)289-4841	(775)289-1565
Ely	NV	89301	(775)289-4811	(775)289-1542
Lund	NV	89317	(775)289-5200	(775)238-0208
Ely	NV	89301	(775)289-2999	(775)289-1592
Ely	NV	89301	(775)289-2999	(775)289-1592
Ely	NV	89301	(775)289-4851x7101	
Ely	NV	89301	(775)289-4811x5110	(775)289-1542
North Las Vegas	NV	89081	(702)533-1896	(702)982-3991
North Las Vegas	NV	89031	(702)342-0880	(702)342-0881
Henderson	NV	89011	(702)846-2310	(480)452-0352
Las Vegas	NV	89113	(702)637-1776	(702)765-0525
Las Vegas	NV	89110	(702)331-5515	
Reno	NV	89512	(775)470-8950	(775)470-8952
Las Vegas	NV	89119	(702)486-6068	
Las Vegas	NV	89119	(702)486-6068	
Las Vegas	NV	89119	(702)486-6068	
Las Vegas	NV	89119	(702)486-6068	
Las Vegas	NV	89119	(702)486-6068	
Las Vegas	NV	89119	(702)486-6068	
Las Vegas	NV	89119	(702)486-6068	
Las Vegas	NV	89119	(702)486-6068	
Las Vegas	NV	89119	(702)668-4348	
			(702)486-6068	
			(702)486-6068	
Las Vegas	NV	89119	(702)668-4348	
Las Vegas	NV	89119	(702)486-6068	
Las Vegas	NV	89106	(702)316-2410	
Henderson	NV	89011	(702)473-5735	(702)473-5753

Las Vegas	NV	89110	(702)907-0432	(702)825-3622
Las Vegas	NV	89115	(725)726-2626	
Las Vegas	NV	89104	(702)550-2876	
Las Vegas	NV	89121	(702)485-2400	(702)485-3322
Las Vegas	NV	89110	(702)478-8318	(702)478-8771
Las Vegas	NV	89110	(702)462-9361	
Las Vegas	NV	89113	(702)970-6800	
Las Vegas	NV	89118	(702)970-6800	
Las Vegas	NV	89130	(702)998-8368	
Las Vegas	NV	89130	(702)350-1472	(702)825-2684
Ely	NV	89301	(775)293-8009	
Las Vegas	NV	89178	(702)960-7500	(702)960-7960
Las Vegas	NV	89128	(702)901-4950	(702)534-7990
Las Vegas	NV	89138	(702)776-8740	(702)826-2636
Las Vegas	NV	89147	(702)776-6491	(702)802-2638
Las Vegas	NV	89139	(702)916-4320	(702)916-4323
Reno	NV	89501	(775)737-4084	(775)437-4533
Henderson	NV	89015	(702)749-3500	(702)749-9995
Henderson	NV	89015	(702)202-2227	(702)202-2393
Henderson	NV	89044	(702)473-5777	(702)754-4355
Las Vegas	NV	89183	(702)750-9150	(702)570-6360
Henderson	NV	89044	(702)462-9700	
Henderson	NV	89015	(702)909-6730	
Las Vegas	NV	89146	(725)500-5295	
North Las Vegas	NV	89084	(702)633-5616	(702)633-5628
North Las Vegas	NV	89081	(702)826-4373	(702)527-7999
Las Vegas	NV	89108	(702)685-9150	(702)722-6906
Las Vegas	NV	89131	(702)478-8888	(702)776-7216
Henderson	NV	89074	(702)998-0500	(702)998-0503
North Las Vegas	NV	89084	(702)916-2327	(702)916-4504
Las Vegas	NV	89166	(702)489-2473	(702)202-0146
Las Vegas	NV	89120	(702)870-5032	
Las Vegas	NV	89121	(702)489-9350	(701)547-5685
Las Vegas	NV	89134	(702)240-0359	(702)240-0432
LAS VEGAS	NV	89108-3541	(702)420-1519	

Las Vegas	NV	89106	(702)638-0222	(702)638-0220
Fallon	NV	89406	(775)423-5437	(775)423-5433
Reno	NV	89511	(775)453-4239	
North Las Vegas	NV	89030	(702)396-2252	(702)396-0848
Elko	NV	89801	(775)738-3422	(775)738-3488
Las Vegas	NV	89104	(702)216-4337	(702)216-4353
Las Vegas	NV	89104	(702)216-4337	(702)216-4353
Las Vegas	NV	89130	(702)631-4751	(702)548-2225
Las Vegas	NV	89149-0210	(702)253-0251	(702)253-0254
North Las Vegas	NV	89032	(702)636-2551	
Sparks	NV	89434	(775)356-1166	(775)356-1168
Las Vegas	NV	89146	(702)257-0578	
Henderson	NV	89014	(702)522-6220	(702)522-6218
Elko	NV	89801	(775)738-5907	(775)738-8812
Las Vegas	NV	89101	(702)953-2600	(702)507-9918
Las Vegas	NV	89146	(702)953-2600	(702)507-9918
Henderson	NV	89074	(702)953-2600	(702)507-9918
Las Vegas	NV	89115	(702)953-2600	(702)507-9918
Las Vegas	NV	89113	(702)953-2600	(702)507-9918
Henderson	NV	89015	(702)953-2600	(702)507-9918
Las Vegas	NV	89130	(702)953-2600	(702)507-9918
North Las Vegas	NV	89031	(702)953-2600	(702)507-9918
Reno	NV	89503	(775)446-7778	
Reno	NV	89521	(775)826-4200	(775)201-0999
Las Vegas	NV	89123	(702)407-1825	(702)407-5055
Las Vegas	NV	89131	(702)685-4333	(702)685-7525
Las Vegas	NV	89115	(702)643-5121	(702)643-5138
Henderson	NV	89052	(702)776-8800	(702)776-8803
Las Vegas	NV	89123	(702)269-8512	(702)269-3258
Henderson	NV	89074	(702)485-3410	(702)722-2718
Henderson	NV	89011	(702)489-9797	(702)489-9191
Henderson	NV	89011	(702)665-6998	(702)462-2773
Las Vegas	NV	89147	(702)726-8600	(702)538-9500
Las Vegas	NV	89169	(702)323-4524	
Las Vegas	NV	89110	(702)224-2771	

Las Vegas	NV	89107	(702)844-8854	
Las Vegas	NV	89130	(702)291-8741	
Elko	NV	89801	(775)860-4300	
Las Vegas	NV	89030	(702)489-4886	
Reno	NV	89511	(702)953-2600	(702)507-9918
Henderson	NV	89015	(702)224-2809	
Sparks	NV	89441	(775)376-1444	
North Las Vegas	NV	89032	(702)483-6332	
North Las Vegas	NV	89030	(702)462-9653	
Las Vegas	NV	89121	(702)931-9972	
Las Vegas	NV	89101	(702)463-0222	
Las Vegas	NV	89156	(702)603-6770	
Henderson	NV	89074		

[illegible]

<https://treembears.org>

<http://schools.ccsd.net/dailey/>

<http://schools.ccsd.net/jlbowler>

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

https://ges.dcsd.net/
https://zces.dcsd.net/
https://jves.dcsd.net/
https://ses.dcsd.net/
https://phes.dcsd.net/
https://mes.dcsd.net/
https://cvms.dcsd.net/
https://pwl.dcsd.net/
https://dhs.dcsd.net/
https://whs.dcsd.net/
https://aspire.dcsd.net/
http://douglasadulter.weebly.com/
https://dcsd.net/
https://www.ecsdnv.net/o/ecsd/page/rural-schools
https://jackpot.ecsdnv.net/
https://www.ecsdnv.net/o/ecsd/page/rural-schools
https://www.ecsdnv.net/o/ecsd/page/rural-schools
https://www.ecsdnv.net/o/ecsd/page/rural-schools
https://liberty.ecsdnv.net/
https://grammar.ecsdnv.net
https://northside.ecsdnv.net/
https://southside.ecsdnv.net/
https://carlin.ecsdnv.net/
https://owyhee.ecsdnv.net/
https://wells.ecsdnv.net/
https://wwelem.ecsdnv.net/
https://mtnview.ecsdnv.net/
https://scem.ecsdnv.net/
https://sage.ecsdnv.net/

https://flagview.ecsdnv.net
https://carlin.ecsdnv.net/
https://wells.ecsdnv.net/
https://adobe.ecsdnv.net/
https://scms.ecsdnv.net/
https://jackpot.ecsdnv.net/
https://owyhee.ecsdnv.net/
https://wwms.ecsdnv.net/
https://carlin.ecsdnv.net/
https://wells.ecsdnv.net/
https://elkohigh.ecsdnv.net/
https://owyhee.ecsdnv.net/
https://jackpot.ecsdnv.net/
https://schs.ecsdnv.net/
https://wwhs.ecsdnv.net
https://www.ecsdnv.net/page/nnva
https://www.ecsdnv.net/page/adult-education
http://www.gbcnv.edu/child/
https://bbyca.ecsdnv.net/
www.esmeraldcountyschools.com
www.esmeraldcountyschools.com
http://eurekacountycves.ss8.sharpschool.com/
http://eurekacountyss8.sharpschool.com/
http://eurekacountyhs.ss8.sharpschool.com/
https://www.hcsdnv.com/o/rrs
https://www.hcsdnv.com/o/rrs
https://www.hcsdnv.com/o/rrs
https://www.hcsdnv.com/o/rrs
https://www.hcsdnv.com/o/she
https://www.hcsdnv.com/o/mcs
https://www.hcsdnv.com/o/gves
https://www.hcsdnv.com/o/wjhs

https://www.hcsdnv.com/o/mcs
https://www.hcsdnv.com/o/lhs
https://www.hcsdnv.com/o/mcs
http://www.hcsdnv.com/adult-ed
http://bmes.lander.k12.nv.us/
http://bmms.lander.k12.nv.us/
http://bmhs.lander.k12.nv.us/
http://austin.lander.k12.nv.us/
http://lcsdnv.com/schools/elementary-schools/pahranagat-valley/
http://lcsdnv.com/schools/elementary-schools/caliente/
http://lcsdnv.com/schools/elementary-schools/panaca/
http://lcsdnv.com/schools/elementary-schools/pioche/
http://lcsdnv.com/schools/middle-schools/meadow-valley/
http://lcsdnv.com/schools/middle-schools/pahranagat-valley/
http://lcsdnv.com/schools/high-schools/lincoln-county/
http://lcsdnv.com/schools/high-schools/pahranagat-valley/
http://lcsdnv.com/schools/high-schools/c-o-bastian-high-school/
http://lcsdnv.com/
http://lcsdnv.com/
https://www.des.lyoncsd.org
https://www.yes.lyoncsd.org
https://www.fes.lyoncsd.org
https://www.sses.lyoncsd.org
https://www.eves.lyoncsd.org
https://www.dis.lyoncsd.org
https://www.ces.lyoncsd.org
https://www.ses.lyoncsd.org
https://www.res.lyoncsd.org
https://www.yis.lyoncsd.org
https://www.fis.lyoncsd.org
https://www.ssms.lyoncsd.org
https://www.sms.lyoncsd.org
https://www.fhs.lyoncsd.org

https://www.svs.lyoncsd.org
https://www.yhs.lyoncsd.org
https://www.dhs.lyoncsd.org
https://www.sshs.lyoncsd.org
https://www.nvmcsd.org/our-schools/hawthorne-elementary
https://www.nvmcsd.org/our-schools/schurz-elementary
https://www.nvmcsd.org/our-schools/hawthorne-junior-high-school
https://www.nvmcsd.org/our-schools/mineral-county-high-school
https://www.nvmcsd.org/our-schools/adult-education
http://manse.nye.k12.nv.us/
http://rndmtn-es.nye.k12.nv.us/
http://gabbs.nye.k12.nv.us/
http://amargosa.nye.k12.nv.us/
http://jgjohnson.nye.k12.nv.us/
http://beatty-ems.nye.k12.nv.us/
http://tonopah-ems.nye.k12.nv.us/
http://mces.nye.k12.nv.us/
http://hafen.nye.k12.nv.us/
http://floyd.nye.k12.nv.us/
http://rclarke.nye.k12.nv.us/
http://beatty-ems.nye.k12.nv.us/
http://tonopah-ems.nye.k12.nv.us/
http://rndmtn-js-hs.nye.k12.nv.us/
http://gabbs.nye.k12.nv.us/
http://amargosa.nye.k12.nv.us/
http://beatty-hs.nye.k12.nv.us/
http://gabbs.nye.k12.nv.us/
http://tonopah-hs.nye.k12.nv.us/
http://pvalley-hs.nye.k12.nv.us/
http://rndmtn-js-hs.nye.k12.nv.us/
http://pathways.nye.k12.nv.us/

http://pathways.nye.k12.nv.us/
http://pathways.nye.k12.nv.us/
http://adulthood.nye.k12.nv.us/
HTTP://BORDEWICH.CARSONCITYSCHOOLS.COM/
HTTP://WWW.CARSONCITYSCHOOLS.COM/DEPARTMENTS/ADULT
HTTP://FRITSCH.CARSONCITYSCHOOLS.COM/
HTTP://FREMONT.CARSONCITYSCHOOLS.COM/
HTTP://SEELIGER.CARSONCITYSCHOOLS.COM/
HTTP://EMPIRE.CARSONCITYSCHOOLS.COM/
HTTP://MARKTWAIN.CARSONCITYSCHOOLS.COM/
CARSONMONTESSORI.COM
HTTP://CMS.CARSONCITYSCHOOLS.COM/
HTTP://EVMS.CARSONCITYSCHOOLS.COM/
HTTP://CARSONHIGH.COM/NEW/MAIN/
www.pcsdnv.com
www.pcsdnv.com
www.pcsdnv.com
www.pcsdnv.com
www.pcdnv.com
https://www.washoeschools.net/anderson
https://www.washoeschools.net/loder
https://www.washoeschools.net/elmcrest
https://www.washoeschools.net/duncan
https://www.washoeschools.net/warner
https://www.washoeschools.net/hunterlake
https://www.washoeschools.net/beck
https://www.washoeschools.net/booth
https://www.washoeschools.net/towles
https://www.washoeschools.net/melton
https://www.washoeschools.net/mountrose

https://www.washoeschools.net/doublediamond
https://www.washoeschools.net/peavine
https://www.washoeschools.net/cannan
https://www.washoeschools.net/corbett
https://www.washoeschools.net/gomm
https://www.washoeschools.net/smithridge
https://stead.washoeschools.net/
https://www.washoeschools.net/veterans
https://www.washoeschools.net/risley
https://www.washoeschools.net/maxwell
https://www.washoeschools.net/drake
https://www.washoeschools.net/greenbrae
https://www.washoeschools.net/katesmith
https://www.washoeschools.net/juniper
https://www.washoeschools.net/lincolnpark
https://www.washoeschools.net/mitchell
https://www.washoeschools.net/brown
https://www.washoeschools.net/huffaker
https://www.washoeschools.net/lemelson
https://www.washoeschools.net/lemmonvalley
https://www.washoeschools.net/pleasantvalley
https://www.washoeschools.net/sunvalley
https://www.washoeschools.net/verdi
https://www.washoeschools.net/natchez
https://www.washoeschools.net/diedrichsen
https://www.washoeschools.net/dunn
https://www.washoeschools.net/palmer
https://www.washoeschools.net/hall
https://www.washoeschools.net/sepulveda
https://www.washoeschools.net/poulakidas
https://www.washoeschools.net/bohach
https://www.washoeschools.net/inclinees
https://www.washoeschools.net/gomes

https://www.washoeschools.net/lenz
https://www.washoeschools.net/dodson
https://www.washoeschools.net/whitehead
https://www.washoeschools.net/alicesmith
https://www.washoeschools.net/caughlinranch
https://www.washoeschools.net/hiddenvalley
https://www.washoeschools.net/silverlake
https://www.washoeschools.net/westergard
https://www.washoeschools.net/taylor
https://www.washoeschools.net/allen
https://www.washoeschools.net/moss
https://www.washoeschools.net/desertheights
https://www.washoeschools.net/spanishspringses
https://www.washoeschools.net/winnemucca
https://www.washoeschools.net/beasley
https://www.washoeschools.net/donnerrsprings
https://www.washoeschools.net/mathews
https://www.washoeschools.net/hunsberger
https://www.washoeschools.net/bennett
https://www.washoeschools.net/vangorder
https://www.washoeschools.net/clayton
https://www.washoeschools.net/swope
https://www.washoeschools.net/vaughn
https://www.washoeschools.net/traner
https://www.washoeschools.net/dilworth
https://www.washoeschools.net/sparksms
https://www.washoeschools.net/obrien
https://www.washoeschools.net/inclinems
https://www.washoeschools.net/billinghurst
https://www.washoeschools.net/mendive

https://www.washoeschools.net/depoali
https://www.washoeschools.net/shaw
https://www.washoeschools.net/coldsprings
https://www.washoeschools.net/skyranch
https://www.washoeschools.net/desertsdkies
https://www.washoeschools.net/wooster
http://www.rhshuskies.com/
https://www.washoeschools.net/sparkshs
https://www.washoeschools.net/hug
https://www.washoeschools.net/reed
https://www.washoeschools.net/washoeinspire
https://www.washoeschools.net/mcqueen
https://www.washoeschools.net/galena
https://www.washoeschools.net/innovations
https://www.washoeschools.net/gerlach
https://www.washoeschools.net/inclinehs
https://www.washoeschools.net/tmcchs
https://www.washoeschools.net/sshs
https://www.washoeschools.net/northvalleyshs
https://www.washoeschools.net/drhs
https://www.washoeschools.net/aact
https://www.washoeschools.net/Page/355
https://www.washoeschools.net/picollo
https://www.washoeschools.net/turningpoint
https://www.washoeschools.net/rise

https://www.washoeschools.net/northstar
www.whitepine.k12.nv.us
www.whitepine.k12.nv.us
www.whitepine.k12.nv.us
www.whitepine.k12.nv.us
www.whitepine.k12.nv.us
www.whitepine.k12.nv.us
www.whitepine.k12.nv.us
www.whitepine.k12.nv.us
www.whitepine.k12.nv.us
www.whitepine.k12.nv.us
www.freedomclassical.org
https://northvalley.legacytraditional.org/
https://cadence.legacytraditional.org/
https://swlasvegas.legacytraditional.org/
https://futuroacademylv.org/
https://www.maternorthernnevada.org/
https://www.dpacnevada.org
https://www.slamnv.org/

www.equipoacademy.org
https://matercactuspark.org/
www.matersahara.org
http://www.matermountainvista.org/
http://www.materbonanza.org/
https://www.matereastlv.org/
https://amplus.academy/
https://amplus.academy/
https://www.fcalv.net
www.lanv.org
www.elylearningbridge.org
http://www.doralcactus.org/
http://doralfiremesa.org/
http://www.doralredrock.org/splash/index.jsp
https://www.doralsaddle.org/
http://www.doralpebble.org/
www.academyoflit.org
http://pinecresthorizon.org
https://www.pinecrestcadence.org/
http://pinecrestinspirada.org
PinecrestStRose.org
www.pinecrestslancanyon.com
https://www.pinecrestvirtual.org/
https://www.pinecrestsprings.org/
http://www.somersetnlv.org
http://www.somersetlosee.org/
http://www.somersetlonemountain.org/
http://www.somersetskypointe.org/
http://somersetstephanie.org/
https://www.somersetaliente.org/
https://www.somersetskyecanyon.org
https://ekacademy.org/
www.dcslv.org
www.dcslv.org
https://www.dobeartsacademy.org/

https://rainbowdreamsacademy.org/
https://www.oanv.org/
https://www.doralnorthernnevada.org/
https://www.deltaacademylv.com/
http://www.eiaanv.net
https://www.iicsn.org/
https://www.iicsn.org/
www.questlv.com
http://imaginemountainview.org
https://futuresedgeacademy.org/
http://www.alpineacademy.net/
https://odysseyk12.org/
www.SilverSandsMCS.org
N/A
https://nevadastatehs.com/
https://nevadastatehs.com/
https://nevadastatehs.com/
https://nevadastatehs.com/
https://nevadastatehs.com/
https://nevadastatehs.com/
https://nevadastatehs.com/
https://nevadastatehs.com/
https://www.connectionsacademy.com/nevada-virtual-school
https://www.nevadavirtual.org/
http://www.caslv.org/
http://www.caslv.org/
http://www.caslv.org/
http://www.caslv.org/
http://www.caslv.org/
http://www.caslv.org/
http://www.caslv.org/
http://www.caslv.org/
http://www.caslv.org/
www.BANV.org
https://www.wylees.org
https://www.snvtradeshighschool.org/

https://www.thrivepointnevada.com/
https://vegasvistaacademy.org/
https://ncaelko.org/
https://nevadarise.org/
www.nevadastatehs.com
https://www.signatureprep.org/
https://www.pinecrestnnv.org/
https://www.explore.academy/lvs
https://www.civicanv.org/
www.ywlalv.org
https://www.clvstrongstartes.org/
https://www.amsschools.org/
https://kesheracademy.org/

District or School Name	State Public Charter Authority (SPCSA)
Correlation Directory Assignment Code	Assignment/Position Name
Example: 245	MATH
100	KINDERGARTEN
101	FIRST GRADE
102	SECOND GRADE
103	THIRD GRADE
104	FOURTH GRADE
105	FIFTH GRADE
106	SIXTH GRADE
107	SEVENTH GRADE
108	EIGHTH GRADE
109	COMBINED GRADES
110	ART
111	ENGLISH
112	ENGLISH AS A SECOND LANGUAGE
113	BILINGUAL
123	SPANISH
124	MATHEMATICS 6TH GRADE
125	MUSIC
126	PHYSICAL EDUCATION
127	READING
128	SCIENCE
129	ELEMENTARY RESOURCE
130	EARLY CHILDHOOD, NON SP ED K-2ND
131	COMPUTER LITERACY
132	COMPUTER APPLICATIONS
133	COMPUTER PROGRAMMING
135	ALTERNATIVE EDUC ELEM
136	SOCIAL STUDIES
137	EARLY CHILDHOOD PRE-K ONLY
140	HUMANITIES
145	SEX EDUCATION
150	ACADEMIC INTERVENTION
160	KDGRN 1ST
161	KDGRN 1ST 2ND
162	KDGRN 1ST 2ND 3RD
163	KDGRN 1ST 2ND 3RD 4TH
164	KDGRN 1ST 2ND 3RD 4TH 5TH
165	KDGRN 1ST 2ND 3RD 4TH 5TH 6TH
166	1ST AND 2ND GRADES
167	1ST 2ND 3RD

169	1ST 2ND 3RD 4TH 5TH
170	1ST 2ND 3RD 4TH 5TH 6TH
171	2ND AND 3RD GRADES
172	2ND 3RD 4TH
175	3RD 4TH
176	3RD, 4TH, AND 5TH GRADES
177	3RD, 4TH, 5TH AND 6TH GRADES
178	4TH 5TH
179	4TH 5TH 6TH
180	5TH 6TH
181	KDGRTN-8TH NOT RURAL
200	AGRICULTURE
201	ANTHROPOLOGY
202	ART
203	BUSINESS EDUCATION
204	COMPUTER LITERACY
205	COMPUTER PROGRAMMER
206	COMPUTER APPLICATIONS
207	DANCE
208	DRIVER EDUCATION
210	AMERICAN LITERATURE
212	DRAMA/THEATRE
213	ENGLISH
214	ENGLISH COMPOSITION
215	ENGLISH GRAMMAR
216	ENGLISH LITERATURE
218	GENERAL SURVEY LITERATURE (INTRO)
219	JOURNALISM
223	SPEECH
226	ENGLISH AS A SECOND LANGUAGE
227	BILINGUAL
230	ARABIC
231	CHINESE
232	FRENCH
233	GERMAN
234	ITALIAN
235	JAPANESE
236	LATIN
237	RUSSIAN
238	SPANISH
240	HEALTH
241	FAMILY & CONSUMER SCIENCE
242	INDUSTRIAL ARTS
243	AUTOMOTIVE TECHNOLOGY

244	TECHNOLOGY EDUCATION
245	MATH
246	MATH W/CALCULUS
247	MATH MINOR
250	MUSIC
255	PHYSICAL EDUCATION
260	READING (NON-DIAGNOSTIC)
262	JROTC
263	PHYSICAL SCIENCE
264	BIOLOGICAL SCIENCE
265	BIOLOGY
266	BOTANY
267	CHEMISTRY
268	EARTH SCIENCE
270	ELECTRONICS
271	ENGINEERING
272	ENVIRONMENTAL EDUCATION
273	ENVIRONMENTAL SCIENCE
274	GENERAL SCIENCE
275	GEOLOGY
276	PHYSICS
277	PHYSIOLOGY/ANATOMY
278	SPACE SCIENCE
279	ZOOLOGY
280	LIFE SCIENCE
281	PRINCIPLES OF SCIENCE
282	OCEANOGRAPHY
284	SOCIAL STUDIES
285	ECONOMICS
286	ETHNIC STUDIES
287	GEOGRAPHY
288	HISTORY
289	POLITICAL SCIENCE
290	PSYCHOLOGY
291	SOCIOLOGY
292	STUDENT LEADERSHIP
293	ALTERNATIVE EDUCATION
294	ACADEMIC INTERVENTION
295	PUBLICATIONS
296	ADULT EDUCATION
297	LIFE SKILLS
298	BUSINESS ENGLISH
300	AGRICULTURE
302	ART

303	BUSINESS EDUCATION
304	COMPUTER LITERACY
305	COMPUTER PROGRAMMER
306	COMPUTER APPLICATIONS
307	DANCE
312	DRAMA/THEATRE
313	ENGLISH
314	ENGLISH COMPOSITION
316	ENGLISH LITERATURE
319	JOURNALISM
323	SPEECH
326	ENGLISH AS A SECOND LANGUAGE
331	CHINESE
332	FRENCH
333	GERMAN
335	JAPANESE
338	SPANISH
340	HEALTH
341	FAMILY & CONSUMER SCIENCE
342	INDUSTRIAL ARTS
344	TECHNOLOGY EDUCATION
345	MATH
346	MATH W/CALCULUS
347	MATH MINOR
350	MUSIC
355	PHYSICAL EDUCATION
360	READING (NON-DIAGNOSTIC)
363	PHYSICAL SCIENCE
364	BIOLOGICAL SCIENCE
367	CHEMISTRY
368	EARTH SCIENCE
373	ENVIRONMENTAL SCIENCE
374	GENERAL SCIENCE
375	GEOLOGY
378	SPACE SCIENCE
380	LIFE SCIENCE
384	SOCIAL STUDIES
386	ETHNIC STUDIES
387	GEOGRAPHY
388	HISTORY
390	PSYCHOLOGY
392	STUDENT LEADERSHIP
393	ALTERNATIVE EDUCATION
394	ACADEMIC INTERVENTION

395	PUBLICATIONS
397	LIFE SKILLS
398	BUSINESS ENGLISH
400	AGRIC BUS & NATURAL RES OCCUPATIONS
401	AGRICULTURE MECHANICS
404	ORNAMENTAL HORTICULTURE
405	AGRICULTURE RESOURCES
407	WILDLIFE MANAGEMENT
409	ANIMAL SCIENCE/VET. MEDICINE
414	BUSINESS & OFFICE OCCUPATIONS
415	ACCOUNTING, BOOKKEEPING
418	SECRETARIAL SERVICES (INV)
420	NATURAL & RENEWABLE ENERGY RESOURCES
422	COMMUNICATIONS & MEDIA OCCUPATIONS
423	LANDSCAPE
424	NEWSPAPER OCCUPATIONS
425	TELEVISION & TELEGRAPH OCCUPATIONS (INV)
426	RADIO & TELEVISION OCCUPATIONS
427	GREENHOUSE PRODUCTION
428	FINANCIAL LITERACY
429	MARKETING & DISTRIBUTION
431	MARKETING, WORK EXPERIENCE (INV)
432	DISTRIBUTION (INV)
435	ENTREPRENEURSHIP
444	ART OCCUPATIONS COMM PHOTOGRAPHY
446	THEATRE OCCUPATIONS
447	PHOTOGRAPHY OCCUP (INV)
449	HEALTH OCCUPATIONS
451	EMERGENCY MEDICAL SERVICE OCCUPATIONS
452	MEDICAL LABORATORY OCCUPATIONS
453	NURSING OCCUPATIONS
456	SPORTS MEDICINE
457	HOME ECONOMICS RELATED OCCUPATIONS
458	CHILD CARE & GUIDANCE
461	HOME FURNISHINGS & EQUIPMENT (INV)
463	FOOD PRODUCTION & MANAGEMENT
465	CULINARY ARTS
466	HOSPITALITY & RECREATIONAL OCCUPATIONS
467	FOOD SCIENCE & NUTRITION
468	HOTEL & MOTEL OCCUPATIONS (LEISURE HOSPI
474	COSMETOLOGY OCCUPATIONS
479	PUBLIC SERVICE OCCUPATIONS
488	TECHNICAL
489	AERONAUTICAL TECHNOLOGY

490	ARCHITECTURAL TECHNOLOGY
491	ELECTRICAL TECHNOLOGY
492	HEATING AIR COND REFRIGERATION
493	ELECTRONIC TECHNOLOGY
494	ENGINEERING TECHNOLOGY
495	AIRFRAME POWER PLANT
496	SCIENTIFIC DATA PROCESSING OCCUPATIONS
497	DRAFTING
499	TRADE & INDUSTRY OCCUPATIONS
500	AUTOMOTIVE SERVICE OCCUPATIONS
501	DIESEL MECHANICS OCCUPATIONS
502	CONSTRUCTION OCCUPATIONS
503	FABRICATION INSTALLATION & REPAIR OCCUPA
506	GRAPHIC ARTS
508	PRINTING/NEWSPAPER (INV)
509	WELDING
511	ANIMATION & GAME DESIGN
523	OCCUPATIONAL INDUSTRIAL ARTS
524	COMMERCIAL PHOTOGRAPHY
530	AIR TRANSPORTATION
531	POLICE & FIRE SERVICES
532	MICRO COMPUTER MAINT
533	COMPUTER NETWORKING
535	COMPUTER SYST PRGRMG
536	COMPUTER WEBSITE DESGN
537	GRAPHIC DIGITAL ARTS (INV)
544	CARPENTRY
545	CRIMINOLOGY
547	CABINETRY
548	CHILD DEVELOPMENT (INV)
549	CHILD & HUMAN DEVELOPMENT
550	ETHNIC MUSIC
551	CAREERS EDUCATION
552	CRIMINAL JUSTICE
558	ETHNIC DANCE
566	LAW ENFORCEMENT
570	MEDICAL ASSISTANT
575	STAGE AND THEATRE
576	COMPUTER DATA PROCESSING
577	COMPUTER MAINT REPAIR
600	ADAPTED PHYSICAL EDUCATION
601	HEARING IMPAIRED
602	HEALTH IMPAIRMENTS, NOT ORTHOPEDIC
603	EARLY CHILDHOOD DEVELOP DELAYED

604	AUTISM
605	GENERALIST
606	TRAUMATIC BRAIN INJURIES
607	SPECIFIC LEARNING DISABILITIES
608	ORTHOPEDIC IMPAIRMENTS
609	SERIOUSLY EMOTIONALLY DISTURBED
610	INTELLECTUAL DISABILITIES
611	SPEECH & LANGUAGE IMPAIRED
612	VISUALLY IMPAIRED
613	GIFTED AND TALENTED
615	MULTIPLE/DIVERSELY IMPAIRED
616	INTELLECTUAL DISABILITIES
625	AMERICAN SIGN LANGUAGE
632	FOUNDATIONS OF LIFE SKILLS
633	LIFE SKILLS
650	EARLY CHILDHOOD REVERSE INCLUSION
700	ELEMENTARY PRINCIPAL
701	SECONDARY PRINCIPAL
702	K-12 PRINCIPALS
703	PRINCIPAL, OCCUPATIONAL EDUCATION
704	SPECIAL SCHOOL PRINCIPALS
705	ELEMENTARY ASSISTANT PRINCIPAL
706	SECONDARY ASSISTANT PRINCIPAL
707	K-12 ASSISTANT PRINCIPAL
708	ASSISTANT PRINCIPAL, OCCUPATIONAL EDUCATION
709	SPECIAL SCHOOL ASSISTANT PRINCIPAL
710	DIRECTOR/SUPERVISOR, INSTRUCTIONAL
711	DIRECTOR/SUPERVISOR, NON-INSTRUCTIONAL
712	SCHOOL ADMINISTRATOR
719	DEAN - ADMINISTRATIVE
735	LOCAL DISTRICT SUPERINTENDENT
736	DEPUTY SUPERINTENDENT
737	ASSISTANT SUPERINTENDENT
738	ASSOCIATE SUPERINTENDENT
740	ADMINISTRATIVE COORDINATOR
750	STUDENT SUCCESS COORDINATOR
800	COUNSELOR ELEMENTARY
801	COUNSELOR SECONDARY
802	COUNSELOR K-12
803	COUNSELOR, OCCUPATIONAL EDUCATION
804	LIBRARY
805	PSYCHOMETRIST
806	SCHOOL NURSE
807	SCHOOL PSYCHOLOGIST

808	SCHOOL SOCIAL WORKER
809	CONSULTANT ESL
810	DEAN OF STUDENTS - NON-ADMINISTRATIVE
811	CONSULTANT/FAC ELEM
812	CONSULTANT/FAC SEC
813	SPECIAL EDUCATION CONSULTANT/FACILITATOR
814	OCCUPATIONAL THERAPIST
815	PROFESSIONAL DEVELOPMENT/TRAINING
816	SPECIAL SERVICES - HOMEBOUND
817	DEAN - NON ADMINISTRATIVE
818	PHYSICAL THERAPIST
819	AUDIOLOGIST
821	ED. COMPUTER STRATEGIST ELEMENTARY
822	ED. COMPUTER STRATEGIST SECONDARY
823	ED. COMPUTER STRATEGIST MIDDLE SCHOOL
825	READING SPECIALIST DIAGNOSTIC
826	CONSULTANT/FACILTR K-12
830	ORIENTATION & MOBILITY
901	MANUFACTURING TECH.
902	HEALTH INFORMATION MNG.
904	THEATRE TECHNOLOGY
905	VIDEO PRODUCTION
906	ACCOUNTING AND FINANCE
915	GRAPHIC DESIGN
920	BIOMEDICAL SCIENCES
926	DIGITAL GAME DEVELOPMENT
929	EMERGENCY MEDICAL TECH
936	FASHION TEXTILES & DESIGN
958	TEACHING AND TRAINING
2641	FORENSICS
6109	SPECIAL EDUCATION ELEMENTARY K-6
6202	SPECIAL EDUCATION ARTS SECONDARY
6213	SPECIAL EDUCATION ENGLISH SECONDARY
6245	SPECIAL EDUCATION MATH SECONDARY
6284	SPECIAL EDUCATION SOCIAL STUDIES SEC
6302	SP ED ARTS MS 7-8
6313	SPECIAL EDUCATION ENGLISH MS
6345	SPECIAL EDUCATION MATH MS
7109	ESL ELEMENTARY
7213	ESL ENGLISH SECONDARY
7313	ESL ENGLISH MS
7374	ESL SCIENCE MS 7-8
8202	ALT ED ARTS SEC 9-12
8213	ALTERNATIVE EDUCATION ENGLISH SEC

8245	ALTERNATIVE EDUCATION MATH
8274	ALTERNATIVE EDUCATION SCIENCE SEC
8284	ALTERNATIVE EDUCATION SOC. STUDIES SEC
8313	ALTERNATIVE EDUCATION ENGLISH MS
8338	ALTERNATIVE EDUCATION FOREIGN LANG. MS
8345	ALTERNATIVE EDUCATION MATH MS
8374	ALTERNATIVE EDUCATION SCIENCE MS
8384	ALTERNATIVE EDUCATION SOC. STUDIES MS

[illegible]

[illegible]

SECONDARY EDUCATION			
SECONDARY EDUCATION			
SECONDARY EDUCATION			
SECONDARY EDUCATION			
SECONDARY EDUCATION			
SECONDARY EDUCATION			
SECONDARY EDUCATION			
SECONDARY EDUCATION			
SECONDARY EDUCATION			
SECONDARY EDUCATION			
SECONDARY EDUCATION			
SECONDARY EDUCATION			
SECONDARY EDUCATION			
SECONDARY EDUCATION			
SECONDARY EDUCATION			
SECONDARY EDUCATION			
SECONDARY EDUCATION			
SECONDARY EDUCATION			
SECONDARY EDUCATION			
SECONDARY EDUCATION			
SECONDARY EDUCATION			
SECONDARY EDUCATION			
SECONDARY EDUCATION			
SECONDARY EDUCATION			
SECONDARY EDUCATION			
SECONDARY EDUCATION			
SECONDARY EDUCATION			
SECONDARY EDUCATION			
SECONDARY EDUCATION			
SECONDARY EDUCATION			
SECONDARY EDUCATION			
SECONDARY EDUCATION			
SECONDARY EDUCATION			
SECONDARY EDUCATION			
MIDDLE SCHOOL EDUCATION			
MIDDLE SCHOOL EDUCATION			

[illegible]

[illegible]

OCCUPATIONAL EDUCATION			
OCCUPATIONAL EDUCATION			
OCCUPATIONAL EDUCATION			
OCCUPATIONAL EDUCATION			
OCCUPATIONAL EDUCATION			
OCCUPATIONAL EDUCATION			
OCCUPATIONAL EDUCATION			
OCCUPATIONAL EDUCATION			
OCCUPATIONAL EDUCATION			
OCCUPATIONAL EDUCATION			
OCCUPATIONAL EDUCATION			
OCCUPATIONAL EDUCATION			
OCCUPATIONAL EDUCATION			
OCCUPATIONAL EDUCATION			
OCCUPATIONAL EDUCATION			
OCCUPATIONAL EDUCATION			
OCCUPATIONAL EDUCATION			
OCCUPATIONAL EDUCATION			
OCCUPATIONAL EDUCATION			
OCCUPATIONAL EDUCATION			
OCCUPATIONAL EDUCATION			
OCCUPATIONAL EDUCATION			
OCCUPATIONAL EDUCATION			
OCCUPATIONAL EDUCATION			
OCCUPATIONAL EDUCATION			
OCCUPATIONAL EDUCATION			
OCCUPATIONAL EDUCATION			
OCCUPATIONAL EDUCATION			
OCCUPATIONAL EDUCATION			
OCCUPATIONAL EDUCATION			
OCCUPATIONAL EDUCATION			
OCCUPATIONAL EDUCATION			
OCCUPATIONAL EDUCATION			
OCCUPATIONAL EDUCATION			
OCCUPATIONAL EDUCATION			
OCCUPATIONAL EDUCATION			
OCCUPATIONAL EDUCATION			
OCCUPATIONAL EDUCATION			
OCCUPATIONAL EDUCATION			
SPECIAL EDUCATION			
SPECIAL EDUCATION			
SPECIAL EDUCATION			
SPECIAL EDUCATION			

[illegible]

PUPIL/SCHOOL SERVICE PERSONNEL			
PUPIL/SCHOOL SERVICE PERSONNEL			
PUPIL/SCHOOL SERVICE PERSONNEL			
PUPIL/SCHOOL SERVICE PERSONNEL			
PUPIL/SCHOOL SERVICE PERSONNEL			
PUPIL/SCHOOL SERVICE PERSONNEL			
PUPIL/SCHOOL SERVICE PERSONNEL			
PUPIL/SCHOOL SERVICE PERSONNEL			
PUPIL/SCHOOL SERVICE PERSONNEL			
PUPIL/SCHOOL SERVICE PERSONNEL			
PUPIL/SCHOOL SERVICE PERSONNEL			
PUPIL/SCHOOL SERVICE PERSONNEL			
PUPIL/SCHOOL SERVICE PERSONNEL			
PUPIL/SCHOOL SERVICE PERSONNEL			
PUPIL/SCHOOL SERVICE PERSONNEL			
PUPIL/SCHOOL SERVICE PERSONNEL			
PUPIL/SCHOOL SERVICE PERSONNEL			
PUPIL/SCHOOL SERVICE PERSONNEL			
PUPIL/SCHOOL SERVICE PERSONNEL			
PUPIL/SCHOOL SERVICE PERSONNEL			
OCCUPATIONAL EDUCATION			
OCCUPATIONAL EDUCATION			
OCCUPATIONAL EDUCATION			
OCCUPATIONAL EDUCATION			
OCCUPATIONAL EDUCATION			
OCCUPATIONAL EDUCATION			
OCCUPATIONAL EDUCATION			
OCCUPATIONAL EDUCATION			
OCCUPATIONAL EDUCATION			
OCCUPATIONAL EDUCATION			
OCCUPATIONAL EDUCATION			
SECONDARY EDUCATION			
ELEMENTARY EDUCATION			
SECONDARY EDUCATION			
SECONDARY EDUCATION			
SECONDARY EDUCATION			
SECONDARY EDUCATION			
MIDDLE SCHOOL EDUCATION			
MIDDLE SCHOOL EDUCATION			
MIDDLE SCHOOL EDUCATION			
ELEMENTARY EDUCATION			
SECONDARY EDUCATION			
MIDDLE SCHOOL EDUCATION			
MIDDLE SCHOOL EDUCATION			
SECONDARY EDUCATION			
SECONDARY EDUCATION			

[illegible]

District Code	District Name	School Code	Site Code
38	Freedom Classical Academy	38435	435
39	Legacy Traditional School	39438	438
39	Legacy Traditional School	39439	439
39	Legacy Traditional School	39440	440
43	Futuro Academy	43100	100
44	Mater Academy of Northern Nevada	44437	437
46	Democracy Prep	46100	100
46	Democracy Prep	46200	200
46	Democracy Prep	46300	300
47	Sports Leadership and Management	47434	434
48	Equipo Academy	48433	433
49	Mater Academy of Nevada	49432	432
49	Mater Academy of Nevada	49433	433
49	Mater Academy of Nevada	49434	434
50	Amplus Academy	50431	431
50	Amplus Academy	50432	432
51	Founders Academy of Las Vegas	51430	430
52	Leadership Academy of Nevada	52429	429
54	Learning Bridge	54428	428
55	Doral Academy	55200	200
55	Doral Academy	55201	201
55	Doral Academy	55202	202
55	Doral Academy	55203	203
55	Doral Academy	55204	204
57	Honors Academy of Literature	57424	424
58	Pinecrest Academy of Nevada	58422	422
58	Pinecrest Academy of Nevada	58423	423
58	Pinecrest Academy of Nevada	58425	425
58	Pinecrest Academy of Nevada	58427	427
58	Pinecrest Academy of Nevada	58428	428
58	Pinecrest Academy of Nevada	58429	429
58	Pinecrest Academy of Nevada	58430	430
59	Somerset Academy of Las Vegas	59119	119
59	Somerset Academy of Las Vegas	59120	120
59	Somerset Academy of Las Vegas	59121	121
59	Somerset Academy of Las Vegas	59122	122
59	Somerset Academy of Las Vegas	59123	123
59	Somerset Academy of Las Vegas	59124	124
59	Somerset Academy of Las Vegas	59125	125
60	Explore Knowledge Academy	60401	401
61	Discovery Charter School	61415	415

61	Discovery Charter School	61417	417
62	Oasis Academy	62101	101
64	Rainbow Dreams Early Learning Acad	64087	087
65	Oasis Academy	65414	414
66	Doral Academy of Northern Nevada	66436	436
67	The Delta Academy	67201	201
68	Elko Institute for Academic Achievement	68410	410
69	Innovations International Charter School	69101	101
69	Innovations International Charter School	69201	201
72	Quest Academy	72416	416
74	Imagine School Mountain View	74418	418
75	FuturEdge Academy	75401	401
76	Alpine Academy	76412	412
77	Odyssey Charter School	77401	401
78	Silver Sands Montessori	78411	411
81	Nevada State High School	81101	101
81	Nevada State High School	81102	102
81	Nevada State High School	81103	103
81	Nevada State High School	81104	104
81	Nevada State High School	81106	106
81	Nevada State High School	81107	107
81	Nevada State High School	81108	108
81	Nevada State High School	81109	109
85	Nevada Connections Academy	85405	405
86	Nevada Virtual Academy	86404	404
87	Coral Academy of Science Las Vegas	87310	310
87	Coral Academy of Science Las Vegas	87311	311
87	Coral Academy of Science Las Vegas	87312	312
87	Coral Academy of Science Las Vegas	87313	313
87	Coral Academy of Science Las Vegas	87314	314
87	Coral Academy of Science Las Vegas	87315	315
87	Coral Academy of Science Las Vegas	87316	316
89	Beacon Academy of Nevada	89409	409
92	Western Youth Leadership, Engagement	92201	201
95	Southern Nevada Trades High School	95301	301
96	Thrive Point Academy of Nevada	96601	601
97	Vegas Vista Academy	97101	101
98	Nevada Classical Academy	98101	101
101	Nevada Rise Academy	101101	101
102	Nevada Prep	102100	100
104	Nevada State High School II	104101	101
105	Signature Preparatory	105101	101
106	Pinecrest Academy of Northern Nevada	106101	101
107	Explore Academy	107101	101

110	CIVICA Academy	110100	100
111	Sage Collegiate Public Charter Scho	111100	100
113	Young Women's Leadership Academ	113100	100
115	Strong Start Academy	115100	100

SchoolName	School Level	Unfilled Teacher Vacancies	Teaching Positions Filled with Long-Term Substitutes
Freedom Classical Academy K-8	OC		
Legacy Traditional School North Valley	OC		
Legacy Traditional School Cadence	ES		
Legacy Traditional School Southwest Las Vegas	ES		
Futuro Academy Elementary	PK		
Mater Academy of Northern Nevada	PK		
Democracy Prep at Agassi Elementary	HS		
Democracy Prep at Agassi Middle	OC		
Democracy Prep at Agassi High	OC		
Sports Leadership and Management Academy	OC		
Equipo Academy	OC		
Mater Mountain Vista	OC		
Mater Bonanza	OC		
Mater Academy East	ES		
Amplus Durango	OC		
Amplus Rainbow	OC		
Founders Academy of Las Vegas	OC		
Leadership Academy of Nevada	OC		
Learning Bridge	OC		
Doral Academy Cactus	OC		
Doral Academy Fire Mesa	OC		
Doral Academy Red Rock	OC		
Doral Academy Saddle	OC		
Doral Academy West Pebble	OC		
Honors Academy of Literature	OC		
Pinecrest Academy of Nevada Horizon	OC		
Pinecrest Academy of Nevada Cadence	OC		
Pinecrest Academy of Nevada Inspirada	OC		
Pinecrest Academy of Nevada St Rose	OC		
Pinecrest Academy of Nevada Sloan Canyon	OC		
Pinecrest Academy of Nevada Virtual	OC		
Pinecrest Academy of Nevada Springs	OC		
Somerset Academy North Las Vegas	OC		
Somerset Academy Losee	OC		
Somerset Academy Lone Mountain	OC		
Somerset Academy Sky Pointe	OC		
Somerset Academy Stephanie	OC		
Somerset Academy Aliante	OC		
Somerset Academy Skye Canyon	OC		
Explore Knowledge Academy	ES/MS/HS		
Discovery Charter School Sandhill	ES		

Discovery Charter School HillPointe	OC
Do & Be Arts Academy of Excellence	OC
Rainbow Dreams Early Learning Academy	PK/EM/MS/HS
Oasis Academy	OC
Doral Academy of Northern Nevada	HS
The Delta Academy	MS/HS
Elko Institute for Academic Achievement	OC
Innovations International Charger School O	PK/ES
Innovations International Charger School S	HS
Quest Academy Northwest	HS
Imagine School Mountain View	HS
FuturEdge Academy	ES/MS
Alpine Academy High School	HS
Odyssey Charter School	ES/MS/HS
Silver Sands Montessori	HS
Nevada State High School Downtown	HS
Nevada State High School Summerlin	HS
Nevada State High School Henderson	HS
Nevada State High School Sunrise	HS
Nevada State High School Southwest	OC
Nevada State High School Downtown Hende	HS
Nevada State High School Northwest	OC
Nevada State High School North Las Vegas	ES
Nevada Connections Academy	OC
Rainbow Dreams Early Learning Academy	ES
Coral Academy Centennial Hills	ES
Coral Academy Nellis AFB	OC
Coral Academy Sandy Ridge	OC
Coral Academy Tamarus	HS
Coral Academy Windmill	OC
Coral Academy Eastgate	OC
Coral Academy Cadence	OC
Beacon Academy of Nevada	OC
Western Youth Leadership, Engagement, an	MS
Southern Nevada Trades High School	OC
Thrive Point Academy	MS
Vegas Vista Academy	OC
Nevada Classical Academy Elko	ES
NV Rise Academy Charter School	ES
Nevada Prep Charter School	OC
Nevada State High School II Meadowwood	OC
Signature Preparatory	ES
Pinecrest Academy of Northern Nevada	ES
Explore Academy	ES

CIVICA Academy	ES
Sage Collegiate Public Charter School	ES
Young Women's Leadership Academy of La	ES/MS/HS
Strong Start Academy	ES

**Vacancies fill by
Independent
Contractors**

Instructions: Assignment Code Vacancy Data

Please input the information requested in columns D, E, and F for each assignment code in your district/charter

Column D

For each assignment code, enter the total of licensed position(s) that are unfilled; there is no one in the position or it's being filled temporarily by other teachers/admin, other licensed education personnel or multiple substitute teachers. (NRS 385A.220 defines a "teacher" as a person who spends at least of 50%

Column E

For each assignment code, enter the total of licensed position(s) filled by a person who holds a Nevada PK-12 substitute license only; and is expected to fill the position for the long term (more that 20 consecutive days) **Please do not duplicate the numbers from Column G. This column is for long term substitutes**

Column F

For each assignment code, enter the total of licensed position(s) filled by an independent contractor. These FTEs are not employed by the district. They work for an organization that is contracted or are individuals who are contracted to provide services to students.

NOTE: This workbook may not not include all available assignment codes. Please add the assignment code(s) and position names to the spreadsheet as needed. Please refer

Instructions: School Level Vacancy Data:

Please input the information requested in columns G, H, and I for each school in your district/charter

Column G

For each school, enter the total of licensed position(s) that are unfilled; there is no one in the position or it's being filled temporarily by other teachers/admin, other licensed education personnel or multiple substitute teachers. (NRS 385A.220 defines a "teacher" as a person who spends at least of 50% of their work year

Column H

For each school, enter the total of licensed position(s) filled by a person who holds a Nevada PK-12 substitute license only; and is expected to fill the position for the long term (more that 20 consecutive days). **Please do not duplicate the numbers from Column G. This column is for long term substitutes**

Column I

For each school, enter the total of licensed position(s) filled by an independent contractor. These FTEs are not employed by the district. They work for an organization that is contracted or are individuals who are contracted to provide services to students.



Understanding the Premium Audit Process:

Tips and Insights from WCF Insurance

At WCF our mission is to create an excellent insurance experience, and we're committed to making the premium audit process as smooth and effortless as possible. Read on as we break down our approach and share helpful tips and insights including how to prepare, what to expect, and how to avoid large audit invoices.

WHY IS AN AUDIT NECESSARY?

Through the audit process we'll work together to determine a fair and accurate premium, and ensure that we meet state-specific requirements. Our team will answer any questions regarding classification codes, reportable payroll, and other factors related to the premium calculation. We'll work closely with you to wrap up the policy year and finalize premium.

WHERE WILL THE AUDIT TAKE PLACE?

We do both virtual and in-person audits. If done virtually, we'll review your uploaded documents and contact you with any questions. If done in person, we will meet with you at your office. If you have a preference, reach out and we'll coordinate with you to determine the best approach.

WHAT TO EXPECT

During the audit, we'll review the information provided, ask a few questions, calculate final premium, and discuss the results. The primary goal is to determine correct premium and we want you to understand the reasoning behind the refund or invoice. Please ask questions and voice concerns, we're here to help.

WHAT HAPPENS NEXT?

Upon completion of the audit, we'll email the report to you and send an invoice or refund a few days later. On further review, if you disagree with the audit, simply contact us and we'll make any necessary corrections. If we're unable to resolve the disagreement then we'll walk you through the appeal process.

TIPS FOR AVOIDING LARGE AUDIT INVOICES

Accurate payroll estimates: Take time to confirm that the estimated payroll is sufficient and assigned to the correct classification codes. Consider monthly or quarterly reporting if your payroll fluctuates significantly.

Adequate payroll tracking: If the classification codes on your policy allow for a division of payroll, be sure to track the payroll for each type of work and keep records to substantiate your allocation. Remember that estimates or percentages are not allowed.

Subcontractor labor: Money paid to uninsured subcontractors, contractors, and temporary laborers is generally included in the premium basis, so be sure to ask your subcontractors to provide certificates of insurance as evidence of coverage before hiring them.

Payroll inclusions and exclusions: When estimating payroll and when submitting monthly or quarterly payroll reports, be familiar with reportable and excludable payroll

WE'RE HERE TO HELP

At WCF, we will support you throughout the policy period—our premium audit team is here to help! Please reach out with any questions regarding payroll inclusions and exclusions, payroll tracking and reporting, subcontract labor certificate requirements, classification codes, or anything else regarding your premium. We appreciate the trust you've placed in us and are committed to providing you with an excellent experience. Please feel free to contact us anytime, and we'll be happy to assist you in any way we can.

CONTACT US

(385) 351-8305
audit@wcf.com
Chat with us at wcf.com