Criminal Justice Information Service Security Policy Requirements

(This document is part of the CJIS Workbook package, which also includes CJIS Security Policy Template, CJIS Security Policy Workbook, and the Criminal Justice Information Service Compliance on AWS whitepaper.)

March 2017

Notices

This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Contents

CJIS Policy Requirements

This document, delivered as part of the CJIS Workbook package, is meant to be a reference to the CJIS Security Policy Template. Customers (or partners) can use the CJIS Security Policy Template to track their control mappings to the CJIS Security Policy 5.5.

The CJIS Workbook package also contains the CJIS Security Policy Workbook Excel spreadsheet, which consolidates all of the information provided by the CJIS Security Policy Template and CJIS Security Policy Requirements documents into a single format.

For more a more in depth discussion of using AWS as part of a CJIS compliant solution, see the Criminal Justice Information Service Compliance on AWS whitepaper.

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.

> ***Applicable Fed Ramp Controls**: AC-21, CA-1, CA-3, SA-10 (1)*

For more information, see Security at Scale: Governance in AWS.

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.

There may be instances, on an ad-hoc basis, where CJI is authorized for further dissemination to Authorized Recipients not covered by an information exchange agreement with the releasing agency. In these instances, the dissemination of CJI is considered to be secondary dissemination. Law Enforcement and civil agencies shall have a local policy to validate a requestor of CJI as an authorized recipient before disseminating CJI. See Section 5.1.3 for secondary dissemination guidance.

Applicable Fed Ramp Controls: *AC-21, CA-3, SA-2, SA-4, SA-4(1), SA-12(2)*

5.1.1.1 – Information Handling

Procedures for handling and storage of information shall be established to protect that information from unauthorized disclosure, alteration or misuse. Using the requirements in this Policy as a starting point, the procedures shall apply to the handling, processing, storing, and communication of CJI. These procedures apply to the exchange of CJI no matter the form of exchange.

The policies for information handling and protection also apply to using CJI shared with or received from FBI CJIS for noncriminal justice purposes. In general, a noncriminal justice purpose includes the use of criminal history records for purposes authorized by federal or state law other than purposes relating to the administration of criminal justice, including – but not limited to - employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

> ***Applicable Fed Ramp Controls:*** *AC-21, CM-9, CP-6, CP-7, IR-8, PL-2, PM-1*

For more information, see AWS Data Protection FAQ. For AWS information handling resources, see:

- AWS Identity & Access Management (IAM)
- Encrypting Data at Rest
- Controlling Access to EC2 Resources
- Amazon S3 encryption
- AWS Key Management Service

5.1.1.2 – State and Federal Agency User Agreements

Each CSA head or SIB Chief shall execute a signed written user agreement with the FBI CJIS Division stating their willingness to demonstrate conformity with this Policy before accessing and participating in CJIS records information programs. This agreement shall include the standards and sanctions governing utilization of CJIS systems. As coordinated through the particular CSA or SIB Chief, each Interface Agency shall also allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system per authorization of Department of Justice (DOJ) Order 2640.2F. All user agreements with the FBI CJIS Division shall be coordinated with the CSA head.

> ***Applicable Fed Ramp Controls:*** *AC-21, CA-3, SA-2, SA-4, SA-4 (1), SA-12 (2)*

5.1.1.3 – Criminal Justice Agency User Agreements

Any CJA receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA providing the access. 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:

1. Audit.
2. Dissemination.
3. Hit confirmation.
4. Logging.
5. Quality Assurance (QA).
6. Screening (Pre-Employment).
7. Security.
8. Timeliness.
9. Training.
10. Use of the system.
11. Validation.

> ***Applicable Fed Ramp Controls:*** *AC-21, CA-3, SA-2, SA-4, SA-4(1), SA-12(2)*

5.1.1.4 – Interagency and Management Control Agreements

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 inter-agency agreement. The NCJA shall sign and execute a management control agreement (MCA) with the CJA, which stipulates management control of the criminal justice function remains solely with the CJA. The MCA may be a separate document or included with the language of an inter-agency agreement. An example of an NCJA (government) is a city information technology (IT) department.

> ***Applicable Fed Ramp Controls:*** *AC-21, CA-3, SA-2, SA-4, SA-4(1), SA-12(2)*

5.1.1.5 – Private Contractor User Agreements and CJIS Security Addendum

The CJIS Security Addendum is 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 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 CJIS Security Policy, provides for sanctions, and contains such other provisions as the Attorney General may require.

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, and abide by all aspects of the CJIS Security Addendum. The CJIS Security Addendum is presented in Appendix H. Modifications to the CJIS Security Addendum shall be enacted only by the FBI.

1. Private contractors designated to perform criminal justice functions for a CJA shall be eligible for access to CJI. Access shall be permitted pursuant to an agreement that specifically identifies the agency's purpose and scope of providing services for the administration of criminal justice. The agreement between the CJA and the private contractor shall incorporate the CJIS Security Addendum approved by the Director of the FBI, acting for the U.S. Attorney General, as referenced in Title 28 CFR 20.33 (a)(7).
2. Private contractors designated to perform criminal justice functions on behalf of a NCJA (government) shall be eligible for access to CJI. Access shall be permitted pursuant to an agreement that specifically identifies the agency's purpose and scope of providing services for the administration of criminal justice. The agreement between the NCJA and the private contractor shall incorporate the CJIS Security Addendum approved by the Director of the FBI, acting for the U.S. Attorney General, as referenced in Title 28 CFR 20.33 (a)(7).

Applicable Fed Ramp Controls: *AC-21, CA-3, SA-2, SA-4, SA-4(1), SA-12(2)*

5.1.1.6 – Agency User Agreements

A NCJA (public) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, 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. A NCJA (public) receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA/SIB providing the access. An example of a NCJA (public) is a county school board.

A NCJA (private) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, 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. A NCJA (private) receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA, SIB, or authorized agency providing the access. An example of a NCJA (private) is a local bank.

All NCJAs accessing CJI shall be subject to all pertinent areas of the CJIS Security Policy (see Appendix J for supplemental guidance). Each NCJA that directly accesses FBI CJI shall also allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system per authorization of Department of Justice (DOJ) Order 2640.2F.

> ***Applicable Fed Ramp Controls:*** *AC-21, CA-3, SA-2, SA-4, SA-4(1), SA-12(2)*

5.1.1.7 – Outsourcing Standards for Channelers

Channelers designated to request civil fingerprint-based background checks or 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 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.

> ***Applicable Fed Ramp Controls:*** *PE-3, PS-1, PS-2, PS-3, PS-6, PS-7*

5.1.1.8 – 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.

> ***Applicable Fed Ramp Controls:*** *AC-21, CA-3, SA-2, SA-4, SA-4(1), SA-12(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. 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.

> ***Applicable Fed Ramp Controls:*** *RA-3, SA-9, SA-9(1)*

For more information, see:

- Acceptable Use Policy
- Pen testing on AWS
- Security Bulletins

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.

> ***Applicable Fed Ramp Control:*** *RA-3*

For more information, see:

- Service Health Dashboard
- AWS Release Notes
- What's New from AWS

5.1.3 – Secondary Dissemination

If CHRI is released to another authorized agency, and that agency was not part of the releasing agency's primary information exchange agreement(s), the releasing agency shall log such dissemination.

> ***Applicable Fed Ramp Controls:*** *PS-3, PS-6, PS-7*

5.1.4 – Secondary Dissemination of Non-CHRI CJI

If CJI does not contain CHRI and is not part of an information exchange agreement, then it does not need to be logged. Dissemination shall conform to

the local policy validating the requestor of the CJI 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.

> ***Applicable Fed Ramp Controls:*** *PS-3, PS-6, PS-7*

5.2 – Policy Area 2: Security Awareness Training

Basic security awareness training shall be required within six months of initial assignment, and biennially thereafter, for all personnel who have access to CJI. The CSO/SIB may accept the documentation of the completion of security awareness training from another agency. Accepting such documentation from another agency means that the accepting agency assumes the risk that the training may not meet a particular requirement or process required by federal, state, or local laws.

> ***Applicable Fed Ramp Controls:*** *AT-1, AT-2, AT-3, IR-2, PL-4*

5.2.1 – Awareness Topics

A significant number of topics can be mentioned and briefly discussed in any awareness session or campaign. To help further the development and implementation of individual agency security awareness training programs the following baseline guidance is provided.

> ***Applicable Fed Ramp Controls:*** *AT-1, AT-2, AT-3, IR-2, PL-4, PL4(1)*

5.2.1.1 – Level One Security Awareness Training

At a minimum, the following topics shall be addressed as baseline security awareness training for all personnel who have unescorted access to a physically secure location:

1. Individual responsibilities and expected behavior with regard to being in the vicinity of CJI usage and/or terminals.

2. Implications of noncompliance.
3. Incident response (Identify points of contact and individual actions).
4. Visitor control and physical access to spaces—discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity.

Applicable Fed Ramp Controls: *AT-2, AT-3*

5.2.1.2 – Level Two Security Awareness Training

In addition to 5.2.1.1 above, the following topics, at a minimum, shall be addressed as baseline security awareness training for all authorized personnel with access to CJI:

5. Media Protection
6. Protect information subject to confidentiality concerns — hardcopy through destruction.
7. Proper handling and marking of CJI.
8. Threats, vulnerabilities, and risks associated with handling of CJI.
9. Social engineering.
10. Dissemination and destruction.

Applicable Fed Ramp Controls: *AT-2(2), AT-3, PL-4, PL-4(1)*

5.2.1.3 – Level three Security Awareness Training

In addition to 5.2.1.1 and 5.2.1.2 above, the following topics, at a minimum, shall be addressed as baseline security awareness training for all authorized personnel with both physical and logical access to CJI:

1. Rules that describe responsibilities and expected behavior with regard to information system usage.
2. Password usage and management-including creation, frequency of changes, and protection.
3. Protection from viruses, worms, Trojan horses, and other malicious code

4. Unknown email attachments.
5. Web usage- allowed versus prohibited; monitoring of user activity.
6. Spam
7. Physical security – increases in risks to systems and data.
8. Handheld device security issues- address both physical and wireless security issues.
9. Use of encryption and the transmission of sensitive/confidential information over the Internet-address agency policy, procedures, and technical contact for assistance.
10. Laptop security- address both physical and information security issues.
11. Personally owned equipment and software- state whether allowed or not (e.g. copyrights).
12. Access control issues- address least privilege and separation of duties
13. Individual accountability – explain what this means in the agency.
14. Use of acknowledgement statements – passwords, access to systems and data, personal use and gain.
15. Desktop security – discuss use of screensavers, restricting visitors' view of information on screen (mitigating "shoulder surfing"), battery backup devices, allowed access to systems.
16. Protect information subject to confidentiality concerns- in systems, archived, on backup media, and until destroyed.
17. Threats, vulnerabilities, and risks associated with accessing CJIS Service systems and services.

Applicable Fed Ramp Controls: *AT-2(2), AT-3, PL-4, PL-4(1)*

5.2.1.4 – Level Four Security Awareness Training

In addition to 5.2.1.1, 5.2.2.2, and 5.2.1.3 above, the following topics, at a minimum, shall be addressed as baseline security awareness training for all Information Technology personnel (system administrators, security administrators, network administrators, etc.):

1. Protection from viruses, worms, Trojan horses, and other malicious code- scanning and updating systems.
2. Data backup and storage- centralized or decentralized approach.
3. Timely application of system patches – part of configuration management.
4. Access control measures.
5. Network infrastructure protection measures.
6. Spam
7. Physical security – increases in risks to systems and data.
8. Handheld device security issues- address both physical and wireless security issues.
9. Use of encryption and the transmission of sensitive/confidential information over the Internet-address agency policy, procedures, and technical contact for assistance.
10. Laptop security- address both physical and information security issues.
11. Personally-owned equipment and software- state whether allowed or not (e.g. copyrights).
12. Access control issues- address least privilege and separation of duties
13. Individual accountability – explain what this means in the agency.
14. Use of acknowledgement statements – passwords, access to systems and data, personal use and gain.
15. Desktop security – discuss use of screensavers, restricting visitors' view of information on screen (mitigating "shoulder surfing"), battery backup devices, allowed access to systems.
16. Protect information subject to confidentiality concerns- in systems, archived, on backup media, and until destroyed.
17. Threats, vulnerabilities, and risks associated with accessing CJIS Service systems and services.

Applicable Fed Ramp Controls: *AT-2(2), AT-3, PL-4, PL-4(1)*

5.2.2 – Security Training Records

Records of individual basic security awareness training and specific information system security training shall be documented, kept current, and maintained by the CSO/SIB/Compact Officer. Maintenance of training records can be delegated to the local level.

> ***Applicable Fed Ramp Controls:*** *AT-4, PL-4*

5.3 – Policy Area 3: Incident Response

The security risk of both accidental and malicious attacks against government and private agencies, remains persistent in both physical and logical environments. To ensure protection of CJI, agencies shall: (i) establish operational incident handling procedures that include adequate preparation, detection, analysis, containment, recovery, and user response activities; (ii) track, document, and report incidents to appropriate agency officials and/or authorities.

Refer to Section 5.13.5 for additional incident response requirements related to mobile devices used to access CJI.

> ***Applicable Fed Ramp Controls:*** *IR-1, IR-4, IR-5*

For more information, see Incident response in the cloud.

5.3.1 – Reporting Information Security Events

The agency shall promptly report incident information to appropriate authorities. Information security events and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken. Formal event reporting and escalation procedures shall be in place. Wherever feasible, the agency shall employ automated mechanisms to assist in the reporting of security incidents. All employees, contractors and third-party users shall be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of agency assets and are required to report any information

security events and weaknesses as quickly as possible to the designated point of contact.

> ***Applicable Fed Ramp Controls:*** *IR-4 (1), IR-6, IR-6 (1), IR-6 (2), IR-7, IR-7 (1), IR-7 (2), IR-8, PE-17*

5.3.1.1 – FBI CJIS Division Responsibilities

The FBI CJIS Division shall:

1. Manage and maintain the CJIS Division's Computer Security Incident Response Capability (CSIRC).
2. Serve as a central clearing house for all reported intrusion incidents, security alerts, bulletins, and other security-related material.
3. Ensure additional resources for all incidents affecting FBI CJIS Division controlled systems as needed.
4. Disseminate prompt advisories of system threats and operating system vulnerabilities via the security policy resource center on FBI.gov, to include but not limited to: Product Security Bulletins, Virus Bulletins, and Security Clips.
5. Track all reported incidents and/or trends.
6. Monitor the resolution of all incidents.

> ***Applicable Fed Ramp Controls:*** *None.*

Applicable to FBI CJIS Division only.

5.3.1.2 – CSA ISO Responsibilities

The CSA ISO shall:

1. Assign individuals in each state, federal, and international law enforcement organization to be the primary point of contact for interfacing with the FBI CJIS Division concerning incident handling and response.

2. Identify individuals who are responsible for reporting incidents within their area of responsibility.
3. Collect incident information from those individuals for coordination and sharing among other organizations that may or may not be affected by the incident.
4. Develop, implement, and maintain internal incident response procedures and coordinate those procedures with other organizations that may or may not be affected.
5. Collect and disseminate all incident-related information received from the Department of Justice (DOJ), FBI CJIS Division, and other entities to the appropriate local law enforcement POCs within their area.
6. Act as a single POC for their jurisdictional area for requesting incident response assistance.

> ***Applicable Fed Ramp Controls:*** *None.*

Applicable to CSA ISO Responsibilities only.

5.3.2 – Management of Information Security Incidents

A consistent and effective approach shall be applied to the management of information security incidents. Responsibilities and procedures shall be in place to handle information security events and weaknesses effectively once they have been reported.

> ***Applicable Fed Ramp Controls:*** *IR-1, IR-8*

For more information, see AWS Best Practices for DDoS Resiliency.

5.3.2.1 – Incident Handling

The agency shall implement incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. Wherever feasible, the agency shall employ automated mechanisms to support the incident handling process.

Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. The agency should incorporate the lessons learned from ongoing incident handling activities into the incident response procedures and implement the procedures accordingly.

> ***Applicable Fed Ramp Controls:*** *IR-4, IR-4 (1), IR-4 (3), IR-4 (4), IR-8*

For more information, see:

- AWS CloudWatch
- EC2 Describe API
- Amazon Simple Notification Service
- AWS Health Dashboard
- AWS CloudTrail logs
- AWS Config

5.3.2.2 – Collection of Evidence

Where a follow-up action against a person or agency after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

> ***Applicable Fed Ramp Controls:*** *IR-4, IR-4 (1), IR-4 (3), IR-4 (4), IR-8*

5.3.3 – Incident Response Training

The agency shall ensure general incident response roles and responsibilities are included as part of required security awareness training.

> ***Applicable Fed Ramp Controls:*** *IR-2, IR-3*

5.3.4 – Incident Monitoring

The agency shall track and document information system security incidents on an ongoing basis. The CSA ISO shall maintain completed security incident reporting forms until the subsequent FBI triennial audit or until legal action (if warranted) is complete; whichever time-frame is greater.

> ***Applicable Fed Ramp Controls:*** *IR-5*

5.4 – Policy Area 4: Auditing and Accountability

Agencies shall implement audit and accountability controls to increase the probability of authorized users conforming to a prescribed pattern of behavior. Agencies shall carefully assess the inventory of components that compose their information systems to determine which security controls are applicable to the various components.

Auditing controls are typically applied to the components of an information system that provide auditing capability (servers, etc.) and would not necessarily be applied to every user-level workstation within the agency. As technology advances, more powerful and diverse functionality can be found in such devices as personal digital assistants and cellular telephones, which may require the application of security controls in accordance with an agency assessment of risk.

> ***Applicable Fed Ramp Controls:*** *AU-1, AU-2, CM-8, CM-8 (1), CM-8 (4), CM-8 (5), CM-8 (9)*

For more information, see Auditing Security Checklist for Use of AWS.

5.4.1 – Auditable Events and Content (Information Systems)

The agency's information system shall generate audit records for defined events. These defined events include identifying significant events that need to be audited as relevant to the security of the information system. The agency shall specify which information system components carry out auditing activities. Auditing activity can affect information system performance and this issue must

be considered as a separate factor during the acquisition of information systems.

The agency's information system shall produce, at the application and/or operating system level, audit records containing sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. The agency shall periodically review and update the list of agency-defined auditable events. In the event an agency does not use an automated system, manual recording of activities shall still take place.

> ***Applicable Fed Ramp Controls:*** *AC-9, AU-2, AU-2 (3), AU-3, AU-3 (1), AU-6, AU-6(1), AU-6(3), AU-12, CA-7*

For more information, see:

- AWS Security Audit Guideline
- Amazon Resource Names (ARNs)
- AWS CloudTrail
- AWS CloudWatch

5.4.1.1 – Events

The following events shall be logged:

1. Successful and unsuccessful system log-on attempts.
2. Successful and unsuccessful attempts to use:
    - access permission on a user account, file, directory or other system resource;
    - create permission on a user account, file, directory or other system resource;
    - write permission on a user account, file, directory or other system resource;

- delete permission on a user account, file, directory or other system resource;
- change permission on a user account, file, directory or other system resource.

3. Successful and unsuccessful attempts to change account passwords.
4. Successful and unsuccessful actions by privileged accounts.
5. Successful and unsuccessful attempts for users to:
   - access the audit log file;
   - modify the audit log file;
   - destroy the audit log file.

Applicable Fed Ramp Controls: *AC-9, AU-2, AU-12, CA-7*

For more information, see:

- Logging IAM Events with AWS CloudTrail
- Server Access Logging S3
- S3 Bucket logging
- Access Logs Elastic Load Balancer (ELB)

5.4.1.2 – Content

The following content shall be included with every audited event:

1. Date and time of the event.

2. The component of the information system (e.g., software component, hardware component) where the event occurred.

3. Type of event.

4. User/subject identity.

5. Outcome (success or failure) of the event.

> ***Applicable Fed Ramp Controls:*** *AU-12*

For more information, see:

- CloudTrail User Guide
- Monitor OS & Application Log Files

5.4.2 – Response to Audit Processing Failures

The agency's information system shall provide alerts to appropriate agency officials in the event of an audit processing failure. Audit processing failures include, for example: software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

> ***Applicable Fed Ramp Controls:*** *AU-5, AU-5(2)*

For more information, see:

- API operations for CloudTrail

5.4.3 – Audit Monitoring, Analysis, and Reporting

The responsible management official shall designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions. Audit review/analysis shall be conducted at a minimum once a week. The frequency of review/analysis should be increased when the volume of an agency's processing indicates an elevated need for audit review. The agency shall increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to agency

operations, agency assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

> ***Applicable Fed Ramp Controls:*** *AU-6, AU-6(1), AU-6(3), AU-7, CA-7*

For more information, see:

- Web Server Log Analysis
- Web Log Analysis Architecture
- Marketplace Log Analysis
- CloudWatch Log Files

5.4.4 – Time Stamps

The agency's information system shall provide time stamps for use in audit record generation. The time stamps shall include the date and time values generated by the internal system clocks in the audit records. The agency shall synchronize internal information system clocks on an annual basis.

> ***Applicable Fed Ramp Controls:*** *AU-8, AU-8(1)*

For more information, see:

- Setting the Time for Your Linux Instance
- Setting the Time for a Windows Instance

5.4.5 – Protection of Audit Information

The agency's information system shall protect audit information and audit tools from modification, deletion and unauthorized access.

Applicable Fed Ramp Controls: *AU-9, AU-9(4)*

5.4.6 – Audit Record Retention

The agency shall retain audit records for at least one (1) year. Once the minimum retention time period has passed, the agency shall continue to retain audit records until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions.

Applicable Fed Ramp Controls: *AU-4, AU-5(1), AU-9(2), AU-11*

For more information, see:

- Archiving S3 to Glazier
- S3 FAQs

5.4.7 – Logging NCIC and III Transactions

A log shall be maintained for a minimum of one (1) year on all NCIC and III transactions. The III portion of the log shall clearly identify both the operator and the authorized receiving agency. III logs shall also clearly identify the requester and the secondary recipient. The identification on the log shall take the form of a unique identifier that shall remain unique to the individual requester and to the secondary recipient throughout the minimum one-year retention period.

Applicable Fed Ramp Controls: *AU-4, AU-11*

For more information, see Enterprise Splunk Amazon Machine Image (AMI).

5.5 – Policy Area 5: Access Control

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.

Applicable Fed Ramp Controls:

For more information, see Amazon IAM documentation.

5.5.1 – Account Management

The agency shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The agency shall validate information system accounts at least annually and shall document the validation process. The validation and documentation of accounts can be delegated to local agencies.

Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The agency shall identify authorized users of the information system and specify access rights/privileges. The agency shall grant access to the information system based on:

1. Valid need-to-know/need-to-share that is determined by assigned official duties.
2. Satisfaction of all personnel security criteria.

The agency responsible for account creation shall be notified when:

1. A user's information system usage or need-to-know or need-to-share changes.
2. A user is terminated or transferred or associated accounts are removed, disabled, or otherwise secured.

> ***Applicable Fed Ramp Controls:*** *AC-2, AC-5, IR-8*

For more information, see:

- AWS Identity and Access Management (IAM)
- AWS IAM Best Practices

5.5.2 – Access Enforcement

The information system shall enforce assigned authorizations for controlling access to the system and contained information. The information system controls shall restrict access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel.

Explicitly authorized personnel include, for example, security administrators, system and network administrators, and other privileged users with access to system control, monitoring, or administration functions (e.g., information system security officers, maintainers, system programmers).

Access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) shall be employed by agencies to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system.

> ***Applicable Fed Ramp Controls:*** *AC-2, AC-2(1), AC-2(7), AC-3, AC-3(3), AC-3(4), AC-5, AC-6(1), AC-6(2), AC-12(1), SC-23(1), SC-23(3)*

For more information, see:

- S3 Access Control List (ACL) Overview
- Granting IAM Users Required Permissions

5.5.2.1 – Least Privilege

The agency shall approve individual access privileges and shall enforce physical and logical access restrictions associated with changes to the information system; and generate, retain, and review records reflecting all such changes. The agency shall enforce the most restrictive set of rights/privileges or access needed by users for the performance of specified tasks. The agency shall implement least privilege based on specific duties, operations, or information systems as necessary to mitigate risk to CJI. This limits access to CJI to only authorized personnel with the need and the right to know.

Logs of access privilege changes shall be maintained for a minimum of one year or at least equal to the agency's record retention policy – whichever is greater.

> ***Applicable Fed Ramp Controls:*** *AC-2, AC-2(4), AC-2(7), AC-5, AC-6, AC-6(5), AC-6(9), AC-10, RA-5(5)*

For more information, see:

- AWS IAM Best Practices Blog
- AWS IAM Best Practices

5.5.2.2 – System Access Control

Access control mechanisms to enable access to CJI shall be restricted by object (e.g., data set, volumes, files, records) including the ability to read, write, or delete the objects. Access controls shall be in place and operational for all IT systems to:

1. Prevent multiple concurrent active sessions for one user identification, for those applications accessing CJI, unless the agency grants authority based upon operational business needs. Agencies shall document the parameters of the operational business needs for multiple concurrent active sessions.

2. Ensure that only authorized personnel can add, change, or remove component devices, dial-up connections, and remove or alter programs.

> ***Applicable Fed Ramp Controls:*** *AC-2, AC-2(4), AC-2(7), AC-5, AC-6, AC-6(5), AC-6(9), AC-10, RA-5(5)*

For more information, see:

- IAM Roles (Delegation and Federation)
- Managing AWS Access Keys
- Federated Access to AWS Console

5.5.2.3 – Access Control Criteria

Agencies shall control access to CJI based on one or more of the following:

1. Job assignment or function (i.e., the role) of the user seeking access.
2. Physical location.
3. Logical location.
4. Network addresses (e.g., users from sites within a given agency may be permitted greater access than those from outside).
5. Time of day and day of week/month restrictions.

> ***Applicable Fed Ramp Controls:*** *AC-2, AC-2 (4), AC-2(7), AC-5, AC-6, AC-6(5), AC-6(9), AC-10, RA-5(5)*

For more information, see AWS Security Token Service.

5.5.2.4 – Access Control Mechanisms

When setting up access controls, agencies shall use one or more of the following mechanisms:

1. Access Control Lists (ACLs). ACLs are a register of users (including groups, machines, processes) who have been given permission to use a

particular object (system resource) and the types of access they have been permitted.

2. Resource Restrictions. Access to specific functions is restricted by never allowing users to request information, functions, or other resources for which they do not have access. Three major types of resource restrictions are: menus, database views, and network devices.
3. Encryption. Encrypted information can only be decrypted, and therefore read, by those possessing the appropriate cryptographic key. While encryption can provide strong access control, it is accompanied by the need for strong key management. If encryption of stored information is employed as an access enforcement mechanism, the cryptography used is Federal Information Processing Standards (FIPS) 140-2 (as amended) compliant (see Section 5.10.1.2 for encryption requirements).
4. Application Level. In addition to controlling access at the information system level, access enforcement mechanisms are employed at the application level to provide increased information security for the agency.

> ***Applicable Fed Ramp Controls:*** *AC-2, AC-2(4), AC-2(7), AC-5, AC-6, AC-6(5), AC-6(9), AC-10, RA-5(5)*

For more information, see:

- AWS Resource-Level Permissions
- AWS Services integration with IAM
- Managing Access with ACLs
- AWS Key Management Service (KMS)
- Signing AWS API Requests
- Granting Permissions to AWS Applications

5.5.3 – Unsuccessful Login Attempts

Where technically feasible, the system shall enforce a limit of no more than 5 consecutive invalid access attempts by a user (attempting to access CJI or systems with access to CJI). The system shall automatically lock the account/node for a 10-minute time period unless released by an administrator.

> ***Applicable Fed Ramp Controls:*** *AC-7, IA-5 (1)*

For more information, see:

- Setting an Account Password Policy for IAM Users
- Multi-Factor Authentication (MFA) Devices with AWS

5.5.4 – System Use Notification

The information system shall display an approved system use notification message, before granting access, informing potential users of various usages and monitoring rules. The system use notification message shall, at a minimum, provide the following information:

1. The user is 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 may be subject to criminal and/or civil penalties.
4. Use of the system indicates consent to monitoring and recording.

The system use notification message shall provide appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remain on the screen until the user acknowledges the notification and takes explicit actions to log on to the information system.

Privacy and security policies shall be consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidance. System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system. For publicly accessible systems:

- the system use information is available and when appropriate, is displayed before granting access;
- any references to monitoring, recording, or auditing are in keeping with privacy accommodations for such systems that generally prohibit those activities; and
- the notice given to public users of the information system includes a description of the authorized uses of the system.

Applicable Fed Ramp Controls: *AC-8, AC-11(1), AC-22*

For more information, see:

- AWS Notification API
- Amazon Simple Notification Service API
- Invoking Lambda notification functions

5.5.5 – Session Lock

The information system shall prevent further access to the system by initiating a session lock after a maximum of 30 minutes of inactivity, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures. Users shall directly initiate session lock mechanisms to prevent inadvertent viewing when a device is unattended. A session lock is not a substitute for logging out of the information system. In the interest of officer safety, devices that are: (1) part of a police vehicle; or (2) used to perform dispatch functions and located within a physically secure location, are exempt from this requirement. Note: an example of a session lock is a screensaver with password.

Applicable Fed Ramp Controls: *AC-11*

For more information, see:

- AWS AD Connector
- Connecting AD to AWS

5.5.6 – Remote Access

The agency shall authorize, monitor, and control all methods of remote access to the information system. Remote access is any temporary access to an agency's information system by a user (or an information system) communicating temporarily through an external, non-agency-controlled network (e.g., the Internet).

The agency shall employ automated mechanisms to facilitate the monitoring and control of remote access methods. The agency shall control all remote accesses through managed access control points. The agency may permit remote access for privileged functions only for compelling operational needs but shall document the rationale for such access in the security plan for the information system.

> ***Applicable Fed Ramp Controls:*** *AC-17, AC-17(3), AC-17(4), AC-17(6)*

For more information, see:

- Remote Gateway Reference Architecture
- Connecting Windows EC2 Using RDP
- Deploy Remote Desktop Gateway on the AWS Cloud
- AWS Multi-Factor Authentication

5.5.6.1 – Personally Owned Information Systems

A personally owned information system shall not be authorized to access, process, store or transmit CJI unless the agency has established and documented the specific terms and conditions for personally owned information system usage. When bring your own devices (BYOD) are authorized, they shall be controlled using the requirements in Section 5.5.7.3 Cellular.

This control does not apply to the use of personally owned information systems to access agency's information systems and information that are intended for public access (e.g., an agency's public website that contains purely public information).

Applicable Fed Ramp Controls: *AC-17*

5.5.6.2 – Publicly Accessible Computers

Publicly accessible computers shall not be used to access, process, store or transmit CJI. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

Applicable Fed Ramp Controls: *AC-17, AC-22*

5.6 – Policy Area 6: Identification and Authentication

The agency shall identify information system users and processes acting on behalf of users and authenticate the identities of those users or processes as a prerequisite to allowing access to agency information systems or services.

Applicable Fed Ramp Controls:

5.6.1 – Identification Policy and Procedures

Each person who is authorized to store, process, and/or transmit CJI shall be uniquely identified. A unique identification shall also be required for all persons who administer and maintain the system(s) that access CJI or networks leveraged for CJI transit. The unique identification can take the form of a full name, badge number, serial number, or other unique alphanumeric identifier. Agencies shall require users to identify themselves uniquely before the user is allowed to perform any actions on the system. Agencies shall ensure that all user IDs belong to currently authorized users. Identification data shall be kept current by adding new users and disabling and/or deleting former users.

Applicable Fed Ramp Controls: *IA-1, IA-2, IA-2 (5)*

For more information, see:

- IAM Best Practices
- IAM Business Use Cases
- Identities (Users, Groups, and Roles)

5.6.1.1 – 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. 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 P (limited access) ORI shall not use the full access ORI of another agency to conduct an inquiry transaction.

Applicable Fed Ramp Controls: *SC-16*

For more information, see:

- Amazon Resource Names (ARNs) and AWS Service Namespaces
- Monitor AWS ELB Load Balancer
- ELB Access Logs
- Enable Access logging

5.6.2 – Authentication Policy and Procedures

Authentication refers to mechanisms or processes that verify users are valid once they are uniquely identified. The CSA/SIB may develop an authentication strategy, which centralizes oversight but decentralizes the establishment and daily administration of the security measures for access to CJI.

Each individual's identity shall be authenticated at either the local agency, CSA, SIB or Channeler level. The authentication strategy shall be part of the agency's audit for policy compliance. The FBI CJIS Division shall identify and authenticate all individuals who establish direct web-based interactive sessions with FBI CJIS Services. The FBI CJIS Division shall authenticate the ORI of all message-based sessions between the FBI CJIS Division and its customer agencies but will not further authenticate the user nor capture the unique identifier for the originating operator because this function is performed at the local agency, CSA, SIB or Channeler level.

Applicable Fed Ramp Controls: *IA-1, IA-2, IA-2(8), IA-2(9), IA-3*

5.6.2.1 – Standard Authenticators

Authenticators are the something you know, something you are, or something you have part of the identification and authentication process. Examples of standard authenticators include passwords, tokens, biometrics, and personal identification numbers (PIN). Agencies shall not allow the same authenticator (i.e., password, PIN) to be used multiple times on a device or system.

> ***Applicable Fed Ramp Controls:*** *IA-5, IA-5(1), IA-5(5), IA-6*

For more information, see:

- AWS Multi-Factor Authentication
- AWS Security Token Service
- Managing Access Keys for IAM Users

5.6.2.1.1 – Password

Agencies shall follow the secure password attributes, below, to authenticate an individual's unique ID. Passwords shall:

1. Be a minimum length of eight (8) characters on all systems.
2. Not be a dictionary word or proper name.
3. Not be the same as the User ID.
4. Expire within a maximum of 90 calendar days.
5. Not be identical to the previous ten (10) passwords.
6. Not be transmitted in the clear outside the secure location.
7. Not be displayed when entered.

> ***Applicable Fed Ramp Controls:*** *IA-5, IA-5(1), IA-5(4)*

For more information, see:

- Managing AWS account passwords
- Setting an Account Password Policy for IAM Users

5.6.2.1.2 – Personal Identification Number

When agencies implement the use of a PIN as a standard authenticator, the PIN attributes shall follow the guidance in section 5.6.2.1.1 (Password). When agencies utilize a PIN in conjunction with a certificate or token (e.g. key fob with rolling numbers) for the purpose of advanced authentication, agencies shall follow the PIN attributes described below. For example: A user certificate is installed on a smartphone for the purpose of advanced authentication (AA). AS the user that invokes that certificate, a PIN meeting the below attributes shall be used to access the certificate for the AA process:

1. Be a minimum of six (6) digits
2. Have no repeating digits (i.e. 112233)
3. Have no sequential patterns (i.e. 123456)
4. Not be the same as the User ID
5. Expire within a maximum of 365 calendar days
    - If a PIN is used to access a soft certificate which is the second factor of authentication, AND the first factor is a password that complies with the requirements in Section 5.6.2.1.1, then the 365-day expiration can be waived by the CSO.
6. Not be identical to the previous three (3) PINs.
7. Not be transmitted in the clear outside the secure location.
8. Not be displayed when entered.

EXCEPTION: When a PIN is used for local authentication, the only requirement is that it be a minimum of six (6) digits.

> ***Applicable Fed Ramp Controls:*** *IA-5, IA-5(1), IA-5(4)*

For more information, see:

- Managing AWS account passwords
- Setting an Account Password Policy for IAM Users

5.6.2.2 – Advanced Authentication

Advanced Authentication (AA) provides for additional security to the typical user identification and authentication of login ID and password, such as: biometric systems, user-based digital certificates (e.g. public key infrastructure (PKI)), smart cards, software tokens, hardware tokens, paper (inert) tokens, out-of-band authenticators (retrieved via a separate communication service channel – e.g., authenticator is sent on demand via text message, phone call, etc.) or "Risk-based Authentication" that includes a software token element comprised of a number of factors, such as network information, user information, positive device identification (i.e. device forensics, user pattern analysis and user binding), user profiling, and high-risk challenge/response questions.

When user-based certificates are used for authentication purposes, they shall:

1. Be specific to an individual user and not to a particular device.
2. Prohibit multiple users from utilizing the same certificate.
3. Require the user to "activate" that certificate for each use in some manner (e.g., passphrase or user-specific PIN)

> ***Applicable Fed Ramp Controls:*** *IA-2(1), IA-2(2), IA-2(3), IA-2(4), IA-2(11), IA-2(13)IA-3(1), IA-5(2), IA-5(11), MA-4, SC-37, SC-37(1)*

For more information, see:

- Using Multi-Factor Authentication (MFA) in AWS
- AWS Developer Authenticated Identities

5.6.2.2.1 – Advanced Authentication Policy and Rationale

The requirement to use or not use AA is dependent upon the physical, personnel and technical security controls associated with the user location. AA shall not be required for users requesting access to CJI from within the perimeter of a physically secure location (Section 5.9), when the technical security controls have been met (Sections 5.5 and 5.10). Conversely, if the technical security controls have not been met, AA shall be required even if the request for CJI

originates from within a physically secure location. Section 5.6.2.2.2 provides agencies with a decision tree to help guide AA decisions.

The intent of AA is to meet the standards of two-factor authentication. Two-factor authentication employs the use of two of the following three factors of authentication: something you know (e.g. password), something you have (e.g. hard token), something you are (e.g. biometric). The two authentication factors shall be unique (i.e. password/token or biometric/password but not password/password or token/token).

INTERIM COMPLIANCE:

1. For interim compliance, users accessing CJI from devices associated with, and located within, a police vehicle are exempt from the AA requirement until September 30, 2014 if the information system being used has not been procured or upgraded any time after September 30, 2005. For the purposes of this Policy, a police vehicle is defined as an enclosed criminal justice conveyance with the capability to comply, during operational periods, with Section 5.9.1.3.
2. Internet Protocol Security (IPSec) does not meet the 2011 requirements for advanced authentication; however, agencies that have funded/implemented IPSec in order to meet the AA requirements of CJIS Security Policy v.4.5 may continue to utilize IPSec for AA until September 30, 2014. Examples:
    - A police officer runs a query for CJI from his/her laptop mounted in a police vehicle. The police officer leverages a cellular network as the transmission medium; authenticates the device using IPSec key exchange; and tunnels across the cellular network using the IPSec virtual private network (VPN). IPSec was funded and installed in order to meet the AA requirements of CJIS Security Policy version 4.5. AA requirements are waived until September 30, 2014.
    - A detective accesses CJI from various locations while investigating a crime scene. The detective uses an agency-managed laptop with IPSec installed and leverages a cellular network as the transmission medium. IPSec was funded and installed in order to meet the AA requirements of CJIS Security Policy version 4.5. AA requirements are waived until September 30, 2014.

EXCEPTION:

AA shall be required when the requested service has built AA into its processes and requires a user to provide AA before granting access. EXAMPLES:

- A user, irrespective of his/her location, accesses the LEO website. The LEO has AA built into its services and requires AA prior to granting access. AA is required.
- A user, irrespective of their location, accesses a State's portal through which access to CJI is facilitated. The State Portal has AA built into its processes and requires AA prior to granting access. AA is required.

> ***Applicable Fed Ramp Controls:*** *IA-2(1), IA-2(2), IA-2(3), IA-2(4), IA-2(11), IA-3(1), IA-5(2), IA-5(11), MA-4*

For more information, see:

- Managing Federation in AWS
- External Identity Providers
- Amazon Cognito Identity
- Adding a Hardware Virtual Private Gateway to Your VPC
- AWS VPN CloudHub

5.6.2.2.2 – Advanced Authentication Decision Tree

The following AA Decision Tree, coupled with figures 9 and 10 below, assist decision makers in determining whether or not AA is required.

1. Can request's originating location be determined physically?

   If either (a) or (b) below are true, the answer to the above question is "yes". Proceed to question 2.

   a. The IP address is attributed to a physical structure; or

   b. The mnemonic is attributed to a specific device assigned to a specific location that is a physical structure.

If neither (a) or (b) above are true, then the answer is “no”. Skip to question number 4.

2. Does request originate from within a physically secure location (that is not a police vehicle) as described in Section 5.9.1?

   If either (a) or (b) below are true, the answer to the above question is “yes”. Proceed to question 3.

   a. The IP address is attributed to a physically secure location; or

   b. If a mnemonic is used it is attributed to a specific device assigned to a specific physically secure location.

   If neither (a) or (b) above are true, then the answer is “no”. Decision tree completed. AA required.

3. Are all required technical controls implemented at this location or at the controlling agency?

   If either (a) or (b) below are true, the answer to the above question is “yes”. Decision tree completed. AA requirement waived.

   a. Appropriate technical controls listed in Sections 5.5 and 5.10 are implemented; or

   b. The controlling agency (i.e. parent agency or agency leveraged as conduit to CJI) extends its wide area network controls down to the requesting agency and the extended controls provide assurance equal or greater to the controls listed in Sections 5.5 and 5.10.

   If neither (a) or (b) above are true, then the answer is “no”. Decision tree completed. AA required.

4. Does request originate from an agency-managed user device?

   If either (a) or (b) below are true, the answer to the above question is “yes”. Proceed to question 5.

   a. The static IP address or MAC address can be traced to registered device; or

   b. Certificates are issued to agency managed devices only and certificate exchange is allowed only between authentication server and agency issued devices.

If neither (a) or (b) above are true, then the answer is “no”. Decision tree completed. AA required.

5. Is the agency managed user device associated with and located within a law enforcement conveyance?

   If any of the (a), (b), or (c) statements below is true the answer to the above question is “yes”. Proceed to question 6.

   c. The static IP address or MAC address is associated with a device associated with a law enforcement conveyance; or

   d. The certificate presented is associated with a device associated with a law enforcement conveyance; or

   e. The mnemonic presented is associated with a specific device assigned and that device is attributed to a law enforcement conveyance.

   If none of the (a), (b), or (c) statements above are true then the answer is “no”. Skip to question number 7.

6. Has there been an acquisition or upgrade since 2005?

   If any of the (a), (b), (c), or (d) statements below are true the answer to the above question is “yes”. Proceed to question number 7.

   a. The “green-screen” MDTs have been replaced with laptops or other mobile devices; or

   b. An upgrade of technology exceeding 25% of the cost of the system being upgraded has taken place; or

   c. Any upgrade to the system encryption module has taken place; or

   d. Any upgrade to the system that is not replacing like technology has taken place.

   If none of the (a), (b), (c), or (d) statements above are true then the answer is “no”. Decision tree completed. AA requirement waived.

7. Was IPSec implemented to meet the requirements of Policy Version 4.5?

   If either (a) or (b) below are true, the answer to the above question is “yes”. Decision tree completed. AA requirement is waived.

   a. The budget acquisition of IPSec was completed prior to January 1, 2009 and IPSec was subsequently implemented; or

b. Implementation of IPSec was completed prior to January 1, 2009.

If neither (a) or (b) above are true, then the answer is "no". Decision tree completed. AA required.

For more information, see:

- Managing Federation in AWS
- External Identity Providers
- Amazon Cognito Identity
- Adding a Hardware Virtual Private Gateway to Your VPC
- AWS VPN CloudHub

5.6.3 – Identifier and Authenticator Management

The agency shall establish identifier and authenticator management processes.

> ***Applicable Fed Ramp Controls:*** *IA-4, IA-4(2), IA-4(4), IA-5, IA-5(8), IA-8*

5.6.3.1 – Identifier Management

In order to manage user identifiers, agencies shall:

1. Uniquely identify each user.
2. Verify the identity of each user.
3. Receive authorization to issue a user identifier from an appropriate agency official.
4. Issue the user identifier to the intended party.
5. Disable the user identifier after a specified period of inactivity.
6. Archive user identifiers.

> ***Applicable Fed Ramp Controls:*** *AC-2(3), IA-4, IA-4(2), IA-4(4), IA-5(3), IA-5(8), IA-8*

5.6.3.2 – Authenticator Management

In order to manage information system authenticators, agencies shall:

1. Define initial authenticator content.
2. Establish administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators.
3. Change default authenticators upon information system installation.
4. Change/refresh authenticators periodically.

Information system authenticators include, for example, tokens, user-based PKI certificates, biometrics, passwords, and key cards. Users shall take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and immediately reporting lost or compromised authenticators.

> ***Applicable Fed Ramp Controls:*** *IA-5, IA-5(6), IA-5(8)*

For more information, see:

- AWS IAM Services
- Signing and Authenticating REST API Requests
- Amazon Cognito
- AWS Security Token Service

5.6.4 – Assertions

Identity providers can be leveraged to identify individuals and assert the individual's identity to a service or to a trusted broker who will in turn assert the identity to a service. Assertion mechanisms used to communicate the results of a remote authentication to other parties shall be:

1. Digitally signed by a trusted entity (e.g., the identity provider).

2. Obtained directly from a trusted entity (e.g. trusted broker) using a protocol where the trusted entity authenticates to the relying party using a secure protocol (e.g. transport layer security [TLS]) that cryptographically authenticates the verifier and protects the assertion.

Assertions generated by a verifier shall expire after 12 hours and shall not be accepted thereafter by the relying party.

> ***Applicable Fed Ramp Controls:*** *IA-2 (12), IA-8 (1), IA-8 (2), IA-8 (3)*

For more information, see:

- Working with Server Certificates
- SSL Certificates for Elastic Load Balancing
- Install and Configure OpenSSL

5.7 – Policy Area 7: Configuration Management

> ***Applicable Fed Ramp Controls:***

5.7.1 – Access Restrictions for Changes

Planned or unplanned changes to the hardware, software, and/or firmware components of the information system can have significant effects on the overall security of the system. The goal is to allow only qualified and authorized individuals access to information system components for purposes of initiating changes, including upgrades, and modifications. Section 5.5, Access Control, describes agency requirements for control of privileges and restrictions.

> ***Applicable Fed Ramp Controls:*** *CM-3, CM-3 (2), CM-4, CM-4 (2), CM-5 (5), CM-5 (6), CM-6, CM-9, MA-2, MA-5, SA-10*

For more information, see:

- AWS Config Guide

- ITIL Event Management in the Cloud

5.7.1.1 – Least Functionality

The agency shall configure the application, service, or information system to provide only essential capabilities and shall specifically prohibit and/or restrict the use of specified functions, ports, protocols, and/or services.

> ***Applicable Fed Ramp Controls:*** *CM-2, CM-3, CM-6, CM-7, CM-7(1), CM-7(2), CM-7(3), CM-7(4), CM-7(5), CM-8(3), CM-10, CM-11, SA-4(9), SA-9(2)*

For more information, see Adhere to IAM Best Practices.

5.7.1.2 – Network Diagram

The agency shall ensure that a complete topological drawing depicting the interconnectivity of the agency network, to criminal justice information, systems and services is maintained in a current status. See Appendix C for sample network diagrams. The network topological drawing shall include the following:

1. All communications paths, circuits, and other components used for the interconnection, beginning with the agency-owned system(s) and traversing through all interconnected systems to the agency end-point.
2. The logical location of all components (e.g., firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations). Individual workstations (clients) do not have to be shown; the number of clients is sufficient.
3. "For Official Use Only" (FOUO) markings.
4. The agency name and date (day, month, and year) drawing was created or updated.

> ***Applicable Fed Ramp Controls:*** *CA-3, CA-9, SC-7 (4)*

For more information, see:

- AWS Architecture Center
- AWS Icons for Architecture Diagrams

5.7.2 – Security of Configuration Documentation

The system configuration documentation often contains sensitive details (e.g. descriptions of applications, processes, procedures, data structures, authorization processes, data flow, etc.) Agencies shall protect the system documentation from unauthorized access consistent with the provisions described in Section 5.5 Access Control.

> ***Applicable Fed Ramp Controls:*** *CM-2, CM-5, CM-5 (1), CM-5 (2), CM-8, CM-8 (1), CM-9, SA-5*

5.8 – Policy Area 8: Media Protection

Media protection policy and procedures shall be documented and implemented to ensure that access to electronic and physical media in all forms is restricted to authorized individuals. Procedures shall be defined for securely handling, transporting and storing media.

> ***Applicable Fed Ramp Controls:***

5.8.1 – Media Storage and Access

The agency shall securely store electronic and physical media within physically secure locations or controlled areas. The agency shall restrict access to electronic and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data shall be encrypted per Section 5.10.1.2.

> ***Applicable Fed Ramp Controls:*** *AC-20 (2), CP-6, CP-7, MA-3 (3), MP-2, MP-3, MP-4*

5.8.2 – Media Transport

The agency shall protect and control electronic and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel.

> ***Applicable Fed Ramp Controls:*** *MP-5*

5.8.2.1 – Digital Media in Transit

Controls shall be in place to protect electronic media containing CJI while in transport (physically moved from one location to another) to help prevent compromise of the data. Encryption, as defined in Section 5.10.1.2 of this Policy, is the optimal control during transport; however, if encryption of the data isn't possible then each agency shall institute other controls to ensure the security of the data.

> ***Applicable Fed Ramp Controls:*** *MP-5, MP-5 (4)*

For more information, see AWS Key Management Service.

5.8.2.2 – Physical Media in Transit

The controls and security measures in this document also apply to CJI in physical (printed documents, printed imagery, etc.) form. Physical media shall be protected at the same level as the information would be protected in electronic form.

> ***Applicable Fed Ramp Controls:*** *MP-5*

5.8.3 – Digital Media Sanitization and Disposal

The agency shall sanitize, that is, overwrite at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy

digital media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.

> ***Applicable Fed Ramp Controls:*** *MA-2, MP-6, MP-6(1), MP-6(2), MP-6(3)*

5.8.4 – Disposal of Physical Media

Physical media shall be securely disposed of when no longer required, using formal procedures. Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information compromise by unauthorized individuals. Physical media shall be destroyed by shredding or incineration. Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel.

> ***Applicable Fed Ramp Controls:*** *MP-6*

5.9 – Policy Area 9: Physical Protection

Physical protection policy and procedures shall be documented and implemented to ensure CJI and information system hardware, software, and media are physically protected through access control measures.

> ***Applicable Fed Ramp Controls:***

5.9.1 – Physically Secure Location

A physically secure location is a facility, a criminal justice conveyance, or an area, or a room, or a group of rooms within a facility with both physical and personnel security controls sufficient to protect CJI and associated information systems. The physically secure location is subject to criminal justice agency management control; SIB control; FBI Security addendum; or a combination thereof.

Sections 5.9.1.1 – 5.9.1.8 describe the physical controls required to be considered a physically secure location, while Sections 5.2 and 5.12,

respectively, describe the minimum-security awareness training and personnel security controls required for unescorted access to a physically secure location. Sections 5.5, 5.6.2.2.1, and 5.10 describe the requirements for technical security controls required to access CJI from within the perimeter of a physically secure location without AA.

Applicable Fed Ramp Controls: *PE-1*

5.9.1.1 – Security Perimeter

The perimeter of physically secure location shall be prominently posted and separated from non-secure locations by physical controls. Security perimeters shall be defined, controlled and secured in a manner acceptable to the CSA or SIB.

Applicable Fed Ramp Controls: *PE-1*

5.9.1.2 – Physical Access Authorizations

The agency shall develop and keep current a list of personnel with authorized access to the physically secure location (except for those areas within the permanent facility officially designated as publicly accessible) or shall issue credentials to authorized personnel.

Applicable Fed Ramp Controls: *MA-4(7), MA-5, PE-2, PE-2(1)*

5.9.1.3 – Physical Access Control

The agency shall control all physical access points (except for those areas within the facility officially designated as publicly accessible) and shall verify individual access authorizations before granting access.

Applicable Fed Ramp Controls: *PE-3, PE-3(3)*

5.9.1.4 – Access Control for Transmission Medium

The agency shall control physical access to information system distribution and transmission lines within the physically secure location.

> ***Applicable Fed Ramp Controls:*** *PE-4*

5.9.1.5 – Access Control for Display Medium

The agency shall control physical access to information system devices that display CJI and shall position information system devices in such a way as to prevent unauthorized individuals from accessing and viewing CJI.

> ***Applicable Fed Ramp Controls:*** *PE-5*

5.9.1.6 – Monitoring Physical Access

The agency shall monitor physical access to the information system to detect and respond to physical security incidents.

> ***Applicable Fed Ramp Controls:*** *PE-3, PE-5, PE-6, PE-6(1)*

5.9.1.7 – Visitor Control

The agency shall control physical access by authenticating visitors before authorizing escorted access to the physically secure location (except for those areas designated as publicly accessible). The agency shall escort visitors at all times and monitor visitor activity.

> ***Applicable Fed Ramp Controls:*** *PE-2(3), PE-3*

5.9.1.8 – Delivery and Removal

The agency shall authorize and control information system-related items entering and exiting the physically secure location.

Applicable Fed Ramp Controls: *PE-8*

5.9.2 – Controlled Area

If an agency cannot meet all of the controls required for establishing a physically secure location, but has an operational need to access or store CJI, the agency shall designate an area, a room, or a storage container, as a controlled area for the purpose of day-to-day CJI access or storage.

The agency shall, at a minimum:

1. Limit access to the controlled 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 Section 5.10.1.2 for electronic storage (i.e. data "at rest") of CJI.

Applicable Fed Ramp Controls: *PE-2, PE-5*

5.10 – Policy Area 10: System and Communications Protection and Information Integrity

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 policy for protecting systems and communications infrastructures.

For more information, see:

- AWS Elastic Load Balancers
- Security Groups for Your Load Balancer

5.10.1 – Information Flow Enforcement

The network infrastructure shall control the flow of information between interconnected systems. Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. In other words, controlling how data moves from one place to the next in a secure manner. Examples of controls that are better expressed as flow control than access control (see Section 5.5) are:

1. Prevent CJI from being transmitted unencrypted across the public network.
2. Block outside traffic that claims to be from within the agency.
3. Do not pass any web requests to the public network that are not from the internal web proxy.

Specific examples of flow control enforcement can be found in boundary protection devices (e.g. proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services or provide a packet filtering capability.

> ***Applicable Fed Ramp Controls:*** *AC-4, AC-20, AC-20(1), CA-3, CA-9, IA-5(7), SC-7(4), SC-7(8), SC-7(11), SC-10, SC-15, SC-15(1)*

For more information, see:

- AWS Network and Security
- Security Groups for VPCs
- Network ACLs
- Adding Hardware Virtual Private Gateway to VPC

5.10.1.1 – Boundary Protection

The agency shall:

4. Control access to networks processing CJI.
5. Monitor and control communications at the external boundary of the information system and at key internal boundaries within the system.
6. Ensure any connections to the Internet, other external networks, or information systems occur through controlled interfaces (e.g. proxies, gateways, routers, firewalls, encrypted tunnels). See Section 5.10.4.4 for guidance on personal firewalls.
7. Employ tools and techniques to monitor network events, detect attacks, and provide identification of unauthorized use.
8. Ensure the operational failure of the boundary protection mechanisms do not result in any unauthorized release of information outside of the information system boundary (i.e. the device shall "fail closed" vs. "fail open").
9. Allocate publicly accessible information system components (e.g. public Web servers) to separate sub networks with separate, network interfaces. Publicly accessible information systems residing on a virtual host shall follow the guidance in Section 5.10.3.2 to achieve separation.

> ***Applicable Fed Ramp Controls:*** *AC-20, CA-3(1), CA-3(2), CA-3(5), PE-3(2), SC-5, SC-5(1), SC-5(2), SC-7, SC-7(3), SC-7(4), SC-7(5), SC-7(7), SC-7(8), SC-7(11), SC-7(12), SC-7(13), SC-7(14), SC-7(18), SC-24*

For more information, see:

- VPC Endpoints
- AWS GovCloud Endpoints

5.10.1.2 – Encryption

1. Encryption shall be a minimum of 128 bits.

2. When CJI is transmitted outside the boundary of the physically secure location, the data shall be immediately protected via cryptographic mechanisms (encryption).

   EXCEPTIONS: See Sections 5.5.7.3.2 and 5.10.2.

3. When CJI is at rest (i.e. stored electronically) outside the boundary of the physically secure location, the data shall be protected via cryptographic mechanisms (encryption).

4. When encryption is employed, the cryptographic module used shall be certified to meet FIPS 140-2 standards.

   Note 1: Subsequent versions of approved cryptographic modules that are under current review for FIPS 140-2 compliancy can be used in the interim until certification is complete.

   Note 2: While FIPS 197 (Advanced Encryption Standard) certification is desirable, a FIPS 197 certification alone is insufficient as the certification is for the algorithm only vs. the FIPS 140-2 standard, which certifies the packaging of an implementation.

5. For agencies using public key infrastructure technology, the agency shall develop and implement a certificate policy and certification practice statement for the issuance of public key certificates used in the information system. Registration to receive a public key certificate shall:

   c. Include authorization by a supervisor or a responsible official.

   d. Be accomplished by a secure process that verifies the identity of the certificate holder.

   e. Ensure the certificate is issued to the intended party.

Applicable Fed Ramp Controls: *AC-17(2), IA-7, MA-4(6), SC-8, SC-8(1), SC-8(2), SC-11, SC-12, SC-12(1), SC-12(2), SC-12(3), SC-13, SC-17, SC-28, SC-28(1), SI-7(6)*

Note: AWS requires that every message be authenticated. For API requests using SOAP, messages must be hashed and signed for integrity and non-repudiation. AWS services require that SOAP messages be secured using the WS-Security standard BinarySecurityToken profile, consisting of an X.509 certificate with an RSA public key.

For more information, see Overview of Security Processes.

5.10.1.3 – Intrusion Detection Tools and Techniques

The agency shall implement network-based and/or host-based intrusion detection tools.

The CSA/SIB shall, in addition:

1. Monitor inbound and outbound communications for unusual or unauthorized activities.
2. Send individual intrusion detection logs to a central logging facility where correlation and analysis will be accomplished as a system wide intrusion detection effort.
3. Employ automated tools to support near real-time analysis of events in support of detecting system level attacks.

> ***Applicable Fed Ramp Controls:*** *SC-7(19), SI-4, SI-4(1), SI-4(2), SI-4(4), SI-4(5), SI-4(7), SI-4(9), SI-4(11), SI-4(12), SI-7, SI-7(1), SI-7(7)*

For more information, see Intrusion Detection in the Cloud.

5.10.1.4 – Voice over Internet Protocol

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 lower costs than traditional telephone services and VoIP can be installed in-line with an organization's existing Internet Protocol (IP) services. Among VoIP's risks that have to be considered carefully are: myriad security concerns, cost issues associated with new networking hardware requirements, and overarching quality of service (QoS) factors.

In addition to the security controls described in this document, the following additional controls shall be implemented when an agency deploys VoIP within a network that contains unencrypted CJI:

1. Establish usage restrictions and implementation guidance for VoIP technologies.
2. Change the default administrative password on the IP phones and VoIP switches.
3. Utilize Virtual Local Area Network (VLAN) technologies to segment VoIP traffic from data traffic.

Appendix G.2 outlines threats, vulnerabilities, mitigations, and NIST best practices for VoIP.

> ***Applicable Fed Ramp Controls:*** *SC-19*

5.10.1.5 – Cloud Computing

Organizations transitioning to a cloud environment are presented unique opportunities and challenges (e.g., purported cost savings and increased efficiencies versus a loss of control over the data). Reviewing the cloud computing white paper (Appendix G.3), the cloud assessment located within the security policy resource center on FBI.gov, NIST Special Publications (800-144, 800-145, and 800-146), as well as the cloud provider's policies and capabilities will enable organizations to make informed decisions on whether or not the cloud provider can offer service that maintains compliance with the requirements of the CJIS Security Policy. The metadata derived from CJI shall not be used by any cloud service provider for any purposes. The cloud service provider shall be prohibited from scanning any email or data files for the purpose of building analytics, data mining, advertising, or improving the services provided.

> ***Applicable Fed Ramp Controls:*** *AC-17, AC-17(1), AC-17(2), AC-17(3), AC-17(4), AC-23, CP-1, CP-2(1),CP-2(3), CP-2(8), CP-6(1), CP-6(3), CP-7, CP-9, CP-10, CP-10(2), IA-1, IA-2, IR-1, IR-6, IR-8, IR-9, MA-1, MA-5, MA-5(4), MP-1, MP-2, MP-4, MP-5, MP-6, MP-7, MP-1(1), PE-1, PE-2, PE-3, PE-18, PL-1, PL-2, PL-2(3), PL-4, PL-4(1), PL-7, PL-8, PL-9, PS-1, PS-3, PS-7, SC-2, SC-2(1), SC-3, SC-4, SC-5, SC-5(1), SC-5(2), SC-5(3), SC-6, SC-7, SC-8, SC-9, SC-12, SC-13, SC-13(1), SC-16, SC-16(1), SC-20, SC-21, SC-22, SC-23, SC-28, SC-28(1), SC-28(2), SC-32, SC-36, SC-38, SC-43, SI-1*

5.10.2 – Facsimile Transmission of CJI

CJI transmitted via a single or multi-function device over a standard telephone line is exempt from encryption requirements. CJI transmitted external to a physically secure location using a facsimile server, application, or service which implements email-like technology, shall meet the encryption requirements for CJI in transit as defined in Section 5.10.

Applicable Fed Ramp Controls: *N/A*

5.10.3 – Partitioning and Virtualization

As resources grow scarce, agencies are increasing the centralization of applications, services, and system administration. Advanced software now provides the ability to create virtual machines that allows agencies to reduce the amount of hardware needed. Although the concepts of partitioning and virtualization existed previously, the need for securing the partitions and virtualized machines has evolved due to the increasing amount of distributed processing and federated information sources now available across the Internet.

Applicable Fed Ramp Controls: *SC-2, SC-4*

For more information, see:

- Amazon Virtual Private Cloud
- Expanding a Linux Partition
- Linux AMI Virtualization Types

5.10.3.1 – Partitioning

The application, service, or information system shall separate user functionality (including user interface services) from information system management functionality.

The application, service, or information system shall physically or logically separate user interface services (e.g. public web pages) from information

storage and management services (e.g. database management). Separation may be accomplished through the use of one or more of the following:

1. Different computers.
2. Different central processing units.
3. Different instances of the operating system.
4. Different network addresses.
5. Other methods approved by the FBI CJIS ISO.

> ***Applicable Fed Ramp Controls:*** *SC-2, SC-2 (1), SC-3, SC-4, SC-32*

For more information, see:

- AWS Regions and Endpoints
- VPC Endpoint for Amazon S3
- Access Control List (ACL) Overview

5.10.3.2 – Virtualization

Virtualization refers to a methodology of dividing the resources of a computer (hardware and software) into multiple execution environments. Virtualized environments are authorized for criminal justice and noncriminal justice activities. In addition to the security controls described in this Policy, the following additional controls shall be implemented in a virtual environment:

1. Isolate the host from the virtual machine. In other words, virtual machine users cannot access host files, firmware, etc.
2. Maintain audit logs for all virtual machines and hosts and store the logs outside the hosts' virtual environment.
3. Virtual Machines that are Internet facing (web servers, portal servers, etc.) shall be physically separate from Virtual Machines that process CJI internally.
4. Device drivers that are "critical" shall be contained within a separate guest.

The following are additional technical security control best practices and should be implemented wherever feasible:

1. Encrypt network traffic between the virtual machine and host.
2. Implement IDS and IPS monitoring within the virtual machine environment.
3. Virtually firewall each virtual machine from each other (or physically firewall each virtual machine from each other with an application layer firewall) and ensure that only allowed protocols will transact.
4. Segregate the administrative duties for the host.

Appendix G-1 provides some reference and additional background information on virtualization.

> ***Applicable Fed Ramp Controls:*** *SC-2, SC-4*

For more information, see:

- Amazon EC2
- Amazon Machine Images (AMI)
- AMI Types

5.10.4 – System and Information Integrity and Policy Control

> ***Applicable Fed Ramp Controls:*** *N/A*

5.10.4.1 – Patch Management

The agency shall identify applications, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws.

The agency (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor) shall develop and implement a local

policy that ensures prompt installation of newly released security relevant patches, service packs and hot fixes. Local policies should include such items as:

1. Testing of appropriate patches before installation.
2. Rollback capabilities when installing patches, updates, etc.
3. Automatic updates without individual user intervention.
4. Centralized patch management.

Patch requirements discovered during security assessments, continuous monitoring or incident response activities shall also be addressed expeditiously.

> ***Applicable Fed Ramp Controls:*** *CM-3, CM-4, CM-4(1), RA-5, RA-5(1), RA-5(2), RA-5(3), SA-11, SA-11(1), SI-2, SI-2 (2), SI-2(3)*

For more information, see:

- Amazon Machine Images (AMI)
- AWS Windows AMI Version History
- Updating Instance Software

5.10.4.2 – Malicious Code Protection

The agency shall implement malicious code protection that includes automatic updates for all systems with Internet access. Agencies with systems not connected to the Internet shall implement local procedures to ensure malicious code protection is kept current (i.e. most recent update available).

The agency shall employ virus protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses) at critical points throughout the network and on all workstations, servers and mobile computing devices on the network. The agency shall ensure malicious code protection is enabled on all of the aforementioned critical points and information systems and resident scanning is employed.

Applicable Fed Ramp Controls: *MA-3 (2), SI-3, SI-3 (1), SI-3 (2)*

For more information, see:

- AWS Overview of Security Services
- AV protection AWS marketplace

5.10.4.3 – Spam and Spyware Protection

The agency shall implement spam and spyware protection.

The agency shall:

1. Employ spam protection mechanisms at critical information system entry points (e.g. firewalls, electronic mail servers, remote access servers).
2. Employ spyware protection at workstations, servers and mobile computing devices on the network.
3. Use the spam and spyware protection mechanisms to detect and take appropriate action on unsolicited messages and spyware/adware, respectively, transported by electronic mail, electronic mail attachments, Internet accesses, removable media (e.g. diskettes or compact disks) or other removable media as defined in this Policy.

Applicable Fed Ramp Controls: *SI-8, SI-8(1), SI-8(2)*

For more information, see:

- AWS Overview of Security Services
- Spam & Spyware protection on AWS marketplace

5.10.4.4 – Security Alerts and Advisories

The agency shall:

1. Receive information system security alerts/advisories on a regular basis.
2. Issue alerts/advisories to appropriate personnel.
3. Document the types of actions to be taken in response to security alerts/advisories.
4. Take appropriate actions in response.
5. Employ automated mechanisms to make security alert and advisory information available throughout the agency as appropriate.

> ***Applicable Fed Ramp Controls:*** *SI-5, SI-5(1), SI-11*

For more information, see:

- AWS Security Bulletins
- Security Resources

5.10.4.5 – Information Input Restrictions

The agency shall restrict the information input to any connection to FBI CJIS services to authorized personnel only.

Restrictions on personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities.

> ***Applicable Fed Ramp Controls:*** *SI-10, SI-12*

5.11 – Policy Area 11: Formal Audits

Formal audits are conducted to ensure compliance with applicable statutes, regulations and policies.

For more information, see AWS Published Certifications.

5.11.1 – Audits by the FBI CJIS Division

5.11.1.1 – Triennial Compliance Audits by the FBI CJIS Division

The FBI CJIS Division is authorized to conduct audits, once every three (3) years as a minimum, to assess agency compliance with applicable statutes, regulations and policies. The CJIS Audit Unit (CAU) shall conduct a triennial audit of each CSA in order to verify compliance with applicable statutes, regulations and policies. This audit shall include a sample of CJAs and, in coordination with the SIB, the NCJAs. Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with applicable statutes, regulations and policies. The FBI CJIS Division shall also have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

> ***Applicable Fed Ramp Controls:*** *CA-2, CA-7*

5.11.1.2 – Triennial Security Audits by the FBI CJIS Division

The FBI CJIS Division is authorized to conduct security audits of the CSA and SIB networks and systems, once every three (3) years as a minimum, to assess agency compliance with the CJIS Security Policy. This audit shall include a sample of CJAs and NCJAs. Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with the CJIS Security Policy.

> ***Applicable Fed Ramp Controls:*** *CA-2*

5.11.2 – Audits by the CSA

Each CSA shall:

1. At a minimum, triennially audit all CJAs and NCJAs which have direct access to the state system in order to ensure compliance with applicable statutes, regulations and policies.

2. In coordination with the SIB, establish a process to periodically audit all NCJAs, with access to CJI, in order to ensure compliance with applicable statutes, regulations and policies.
3. Have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.
4. Have the authority, on behalf of another CSA, to conduct a CSP compliance audit of contractor facilities and provide 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: This authority does not apply to the audit requirement outlined in the Security and Management Control Outsourcing Standard for Non-Channel and Channelers related to outsourcing noncriminal justice administrative functions.

Applicable Fed Ramp Controls: *CA-2*

5.11.3 – Special Security Inquiries and Audits

All agencies having access to CJI shall permit an inspection team to conduct an appropriate inquiry and audit of any alleged security violations. The inspection team shall be appointed by the APB and shall include at least one representative of the CJIS Division. All results of the inquiry and audit shall be reported to the APB with appropriate recommendations.

Applicable Fed Ramp Controls: *CA-2, CA-2(1), CA-5, CA-6, CA-7(1), CM-3(4)*

5.12 – Policy Area 12: Personnel Security

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 access to unencrypted CJI including those individuals with only physical or logical access to devices that store, process or transmit unencrypted CJI.

5.12.1 – Personnel Security Policy and Procedure

5.12.1.1 – Minimum Screening Requirements for Individuals Requiring Access to CJI

1. To verify identification, a state of residency and national fingerprint-based record checks shall be conducted within 30 days of assignment for all personnel who have direct access to CJI and those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI. However, if the person resides in a different state than that of the assigned agency, the agency shall conduct state (of the agency) and national fingerprint-based record checks and execute a NLETS CHRI IQ/FQ/AQ query using purpose code C, E, or J depending on the circumstances. When appropriate, the screening shall be consistent with:

    (i) 5 CFR 731.106; and/or

    (ii) Office of Personnel Management policy, regulations, and guidance; and/or

    (iii) agency policy, regulations, and guidance.

    (See Appendix J for applicable guidance regarding noncriminal justice agencies performing adjudication of civil fingerprint submissions.) Federal entities bypassing state repositories in compliance with federal law may not be required to conduct a state fingerprint-based record check.

2. All requests for access shall be made as specified by the CSO. The CSO, or their designee, is authorized to approve access to CJI. All CSO designees shall be from an authorized criminal justice agency.

3. If a felony conviction of any kind exists, the hiring authority in the Interface Agency shall deny access to CJI. However, the hiring authority may ask for a review by the CSO in extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance.

4. If a record of any other kind exists, access to CJI shall not be granted until the CSO or his/her designee reviews the matter to determine if access is appropriate.

5. If the person appears to be a fugitive or has an arrest history without conviction, the CSO or his/her designee shall review the matter to determine if access to CJI is appropriate.
6. If the person is employed by a NCJA, the CSO or his/her designee, and, if applicable, the appropriate board maintaining management control, shall review the matter to determine if CJI access is appropriate. This same procedure applies if this person is found to be a fugitive or has an arrest history without conviction.
7. 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. This does not implicitly grant hiring/firing authority with the CSA, only the authority to grant access to CJI. For offenses other than felonies, the CSO has the latitude to delegate continued access determinations to his or her designee.
8. If the CSO or his/her designee 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.
9. Support personnel, contractors, and custodial workers with access to physically secure locations or controlled areas (during CJI processing) shall be subject to a state and national fingerprint-based record check unless these individuals are escorted by authorized personnel at all times.

It is recommended individual background re-investigations be conducted every five years unless Rap Back is implemented.

Applicable Fed Ramp Controls: *PS-2, PS-3, PS-3 (1), PS-3 (2), PS-3 (3), PS-6, PS-6 (2), PS-7*

5.12.1.2 – Personnel Screening for Contractors and Vendors

In addition to meeting the requirements in paragraph 5.12.1.1, contractors and vendors shall meet the following requirements:

1. Prior to granting access to CJI, the CGA on whose behalf the Contractor is retained shall verify identification via a state of residency and national fingerprint-based record check. However, if the person resides in a

different state than that of the assigned agency, the agency shall conduct state (of the agency) and national fingerprint-based record checks and execute a NLETS CHRI IQ/FQ/AQ query using purpose code C, E, or J depending on the circumstances.

2. If a record of any kind is found, the CGA shall be formally notified and system access shall be delayed pending review of the criminal history record information. The CGA shall in turn notify the Contractor-appointed Security Officer.
3. When identification of the applicant with a criminal history has been established by fingerprint comparison, the CGA or the CJA (if the CGA does not have the authority to view CHRI) shall review the matter.
4. A Contractor employee found to have a criminal record consisting of felony conviction(s) shall be disqualified.
5. Applicants shall also be disqualified on the basis of confirmations that arrest warrants are outstanding for such applicants.
6. The CGA shall maintain a list of personnel who have been authorized access to CJI and shall, upon request, provide a current copy of the access list to the CSO.

Applicants with a record of misdemeanor offense(s) may be granted access if the CSO determines the nature or severity of the misdemeanor offense(s) do not warrant disqualification. The CGA may request the CSO to review a denial-of-access determination.

Applicable Fed Ramp Controls: *PS-2, PS-3, PS-7*

5.12.2 – Personnel Termination

The agency, upon termination of individual employment, shall immediately terminate access to CJI.

Applicable Fed Ramp Controls: *PS-4*

5.12.3 – Personnel Transfer

The agency shall review CJI access authorizations when personnel are reassigned or transferred to other positions within the agency and initiate appropriate actions such as closing and establishing accounts and changing system access authorizations.

> ***Applicable Fed Ramp Controls:*** *PS-5*

5.12.4 – Personnel Sanctions

The agency shall employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.

PS-8

5.13 – Policy Area 13: Mobile Devices

This policy area describes considerations and requirements for mobile devices including smart phones 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 of the Security Policy provides reference material and additional information on mobile devices.

Examples of wireless technologies include, but are not limited to: 802.11x, 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.

5.13.1 – Wireless Communications Technologies

Examples of wireless communications 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.

> ***Applicable Fed Ramp Controls:*** *AC-18, SI-4(14), SI-4(15)*

5.13.1.1 – All 802.11x Wireless Protocols

Agencies shall:

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 Section 5.6.2.1.
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 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 and disable hypertext transfer protocol (HTTP) when not needed or protect HTTP access with authentication and encryption.
13. Enable logging (if supported) and review the logs on a recurring basis per local policy. At a minimum logs shall be reviewed monthly.
14. Segregate, 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.
15. 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.

Applicable Fed Ramp Controls: *AC-18(5), SI-4(15)*

5.13.1.2 – Cellular

Cellular telephones, smartphones (i.e. Blackberry, iPhones, etc.), 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 law enforcement officer).
7. Cloning (not as prevalent with later generation cellular technologies).
8. Server-resident data.

Applicable Fed Ramp Controls: *AC-19, AC-19(5)*

5.13.1.2.1 – Cellular Service Abroad

Certain 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 for use 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.

Applicable Fed Ramp Controls: *AC-19, AC-19(5)*

5.13.1.2.2 – Voice Transmissions Over Cellular Devices

Any cellular device used to transmit CJI via voice is exempt from the encryption and authentication requirements.

Applicable Fed Ramp Controls: *AC-19, AC19(5)*

5.13.1.3 – Bluetooth

Bluetooth is an open standard for short-range radio frequency (RF) communication. 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 know 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. AC-18(5)

5.13.1.4 – 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 device's 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
    - 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. Allow only connections from agency controlled devices

Note: Refer to the requirements in Section 5.10.1.2 encryption for item #1. Refer to the requirements in Section 5.6.2.2.1 Password for item #3. Only password attributes #1, #2, #3 are required.

OR

1. Have a MDM solution to provide the same security as identified in items 1-5.

> ***Applicable Fed Ramp Controls:*** *AC-18, AC-18(1), AC-19, IA-5, IA-5(1), IA-5(4), SC-40, SI-4(14), SI-4(15)*

5.13.2 – Mobile Device Management (MDM)

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 application 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.

Agencies shall implement the following controls when allowing CJI access from cell/smart phones and tablet devices:

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:
    - Remote locking of device
    - ii. Remote wiping of device
    - iii. Setting and locking device configuration
    - iv. Detection of “rooted” and “jailbroken” devices
    - v. Enforce folder or disk level encryption
    - vi. Application of mandatory policy settings on the device

Detection of unauthorized configurations or software/applications

Applicable Fed Ramp Controls: *AC-19, AC-19(5)*

5.13.3 – Wireless Device Risk Mitigations

Organizations shall, at a minimum, ensure that cellular 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 Section 5.10.4.1
2. Are configured for local device authentication (see Section 5.13.9.1).
3. Use advanced authentication.
4. Encrypt all CJI resident on the device.
5. Erase cached information, to include authenticators (see Section 5.6.2.1) in applications, when session is terminated.
6. Employ personal firewalls or run a Mobile Device Management (MDM) system that facilitates the ability to provide firewall services from the agency level.
7. Employ antivirus software or run a MDM system that facilitates the ability to provide antivirus services from the agency level.

Applicable Fed Ramp Controls: *AC-19, AC-19(5)*

5.13.4 – 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.

> ***Applicable Fed Ramp Controls:*** *CM-1, CM-2, CM-2(1), Cm-2(3), CM-2(7), CM-3, CM-3(1), CM-3(2)*

5.13.4.1 – 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 not capable of an "always on" cellular connection (i.e. Wi-Fi only or Wi-Fi with cellular on-demand) to ensure their patch and update state is current.

> ***Applicable Fed Ramp Controls:*** *CM-3, CM-4, CM-4(1), RA-5, RA-5(1), RA-5(2), RA-5(3), SA-11, SA-11(1), SI-2, SI-2(2), SI-2(3)*

5.13.4.2 – 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. An appropriately configured MDM shall be used on smartphones and tablets to prevent the installation of unauthorized software or applications.

> ***Applicable Fed Ramp Controls:*** *MA-3(2), SI-3, SI-3(1), SI-3(2)*

5.13.4.3 – 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 similar functions a personal firewall would provide on a device with a full feature operating system. Appropriately configured MDM software is capable of controlling which applications are allowed on the device.

> ***Applicable Fed Ramp Controls:*** *SC-18, SC-18(1) SC-18(2), SC-18(3), SC-18(4)*

5.13.5 – 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.
    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.
   a. CJI stored on device
   b. Lock state of device
   c. Capabilities for remote tracking or wiping of device
3. Device compromise.
4. Device loss or compromise outside the United States.

> ***Applicable Fed Ramp Controls:*** *IR-1, IR-2, IR-4, IR-8*

5.13.6 – Access Control

Multiple user accounts are not generally supported on limited function mobile operating systems. This may mean the policy requirements for access control (Section 5.5 Access Control, regarding account management) would not apply to the operating system, but rather to a particular application, either stand-alone to the device or as part of a client server architecture.

> ***Applicable Fed Ramp Controls:*** *AC-5, AC-6, AC-6(5), AC-6(9), AC-19, AC-19(5)*

5.13.7 – 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.

> ***Applicable Fed Ramp Controls:*** *IA-1, IA-2, IA-2(1), IA-2(2), IA-2(3), IA-2(4), IA-2(8), IA-2(9), IA-2(11), IA-3, IA-5(2), IA-5(11), MA-4, SC-37, SC-37(1)*

5.13.7.1 – 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 section 5.6.2.1 Standard Authenticators.

> ***Applicable Fed Ramp Controls:*** *IA-1, IA-2, IA-2(5)*

5.13.7.2 – Advanced Authentication

When accessing CJI from an authorized device, advanced authentication shall be used by the authorized user

> ***Applicable Fed Ramp Controls:*** *IA-2(1),IA-2(2), IA-2(3), IA-2(4), IA-2(11), IA-2(13), IA-3(1), IA-5(2), IA-5(11), MA-4, SC-37, SC-37(1)*

5.13.7.2.1 – 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 5.13.2. 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 on upon the existing requirements for AA as compensating controls

Additionally, compensating controls may rely on other, non-AA, existing requirements as compensating controls and/or be combined with new controls to create compensating controls.

The proposed compensating controls for AA are a combination of controls that provide an 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 the reduce the risk of exposure if information is accessed by an unauthorized party.

At least two of the following examples of AA compensating controls for agency-issued smartphones and tablets with limited feature operating systems shall be implemented to qualify for compensating control consideration:

- Possession of the agency-issued smartphone or tablet as an indication it is the authorized user
- Implemented password protection on the Mobile Device Management application and/or secure container where the authentication application is stored
- Enable remote device locking
- Enable remote data deletion
- Enable automatic data wipe after a pre-determined number of failed authentication attempts
- Remote device location (GPS) tracking
- Require CJIS Security Policy compliant password to access the device
- Use of device certificates as per Section 5.13.7.3 Device Certificates

Applicable Fed Ramp Controls: *AC-19, IA-3, IA-3(4), PE-18(1), PE-20*

5.13.7.3 – 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 stored on the device, 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

Applicable Fed Ramp Controls: *AC-19, IA-3, IA3(4)*

Document Revisions

Date	Description
March 2017	Updates to Criminal Justice Information Service Security Policy 5.5.
November 2016	Initial document