



Requirements Companion Document to the FBI CJIS Security Policy Version 5.9.3

09/14/2023



Prepared by:
CJIS Information Security Officer

Recommended changes to version 5.9.2 of the *CJIS Security Policy (CSJISECPOL)* were approved by the Advisory Policy Board (APB) in 2022 and subsequently approved by the Director, FBI. The Policy contains current requirements carried over from previous versions along with newly approved requirements for agencies to implement. New language is indicated in ***black bold italics*** and deleted language is indicated in ~~strikethrough~~.

The “Summary of Changes” page lists the sections with changes. Within the document, modifications are **highlighted in yellow** for ease of location.

The document includes the “Audit / Sanction Date” column. This column indicates the date when modernized security controls will become sanctionable for audit. Current requirements and controls are indicated in **GREEN** and state ‘Current’. New requirements not yet sanctionable are indicated in **YELLOW** with the date they will become auditable and sanctionable. The date format is mm/dd/yyyy.

The document also contains the “cloud matrix” consisting of additional columns describing who (CJIS/CSO, Agency, Cloud Service Provider or both the agency and service provider) has the technical capability to perform the actions necessary to ensure a particular requirement is being met. ***NOTE: The Agency is always ultimately accountable to ensure Policy compliance.*** Three sub-columns are labeled IaaS, PaaS and SaaS and depict the type of cloud services being leveraged by the Agency from the Cloud Service Provider. Respectively, these cloud service models are:

- IaaS – Infrastructure as a Service
- PaaS – Platform as a Service
- SaaS – Software as a Service

Responsibility is color-coded within the columns based on the agreed ability to perform the actions necessary to meet requirements. They are as follows:

| | |
|------------|------------------|
| Dark Gray | CJIS/CSO |
| Dark Green | Agency |
| Dark Blue | Service Provider |
| Orange | Both |

Some modernized controls have not been assigned cloud matrix values and the corresponding cells are blacked out.

Please refer questions or comments about this document or the current version of the *CJISSECPOL* to your respective State CJIS Information Security Officer, CJIS Systems Officer, Compact Officer, or the FBI CJIS ISO at iso@fbi.gov.

SUMMARY OF CHANGES

Version 5.9.3

1. **Section 5.3 Incident Response, Fall 2022, APB#15, SA#4, Modernizing Incident Response (IR) in the CJISSECPOL:** modernize the CJIS Security Policy requirements for *Incident Response Policy and Procedures, Incident Response Training, Incident Response Testing, Incident Handling, Incident Monitoring, Incident Reporting, Incident Response Assistance, and Incident Response Plan.*
2. **Section 5.5 Access Control, Fall 2022, APB#15, SA#3, Modernizing Access Control (AC) in the CJISSECPOL:** modernize the CJIS Security Policy requirements for *Access Control Policy and Procedures, Account Management, Access Enforcement, Information Flow Enforcement, Separation of Duties, Least Privilege, Unsuccessful Logon Attempts, System Use Notification, Device Lock, Session Termination, Remote Access, Wireless Access, Access Control for Mobile Devices, Use of External Systems, Information Sharing, and Publicly Accessible Content.*
3. **Section 5.16 Maintenance, Fall 2022, APB#15, SA#5, Modernizing Maintenance (MA) in the CJISSECPOL:** modernize the CJIS Security Policy requirements for *Maintenance Policy and Procedures, Controlled Maintenance, Maintenance Tools, Nonlocal Maintenance, Maintenance Personnel, and Timely Maintenance.*

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|-----------------------------------------------------------------------------------------------------|----------------------------------------|----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|----------|----------|
| | | | | | IaaS | PaaS | SaaS |
| CJIS Security Policy Sections 1 - 4 (Introduction, Approach, Roles & Responsibilities, and CJI/PII) | | | | | | | |
| 1.3 | 1.3 | Relationship to Local Security Policy and Other Policies | The local agency may complement the CJIS Security Policy with a local policy, or the agency may develop their own stand-alone security policy; however, the CJIS Security Policy shall always be the minimum standard and local policy may augment, or increase the standards,... | Current | Agency | Agency | Agency |
| | | " | ...and local policy may augment, or increase the standards, but shall not detract from the CJIS Security Policy standards. | Current | Agency | Agency | Agency |
| | | " | The agency shall develop, disseminate, and maintain formal, documented procedures to facilitate the implementation of the CJIS Security Policy and, where applicable, the local security policy. | Current | Agency | Agency | Agency |
| | | " | The policies and procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. | Current | Agency | Agency | Agency |
| 3.2.1 | 3.2.1 | CJIS Systems Agencies (CSA) | The head of each CSA shall appoint a CJIS Systems Officer (CSO). | Current | CJIS/CSO | CJIS/CSO | CJIS/CSO |
| | | " | Such decisions shall be documented and kept current. | Current | CJIS/CSO | CJIS/CSO | CJIS/CSO |
| 3.2.1 | 3.2.1 | CJIS Systems Officer (CSO) | Pursuant to The Bylaws for the CJIS Advisory Policy Board and Working Groups, the role of CSO shall not be outsourced. | Current | CJIS/CSO | CJIS/CSO | CJIS/CSO |
| | | " | The CSO shall set, maintain, and enforce the following: | Current | | | |
| 3.2.2(1) | 3.2.2(1) | " | 1. Standards for the selection, supervision, and separation of personnel who have access to CJI. | Current | CJIS/CSO | CJIS/CSO | CJIS/CSO |
| 3.2.2(2) | 3.2.2(2) | " | 2. Policy governing the operation of computers, access devices, circuits, hubs, routers, firewalls, and other components that comprise and support a telecommunications network and related CJIS systems used to process, store, or transmit CJI, guaranteeing the priority, confidentiality, integrity, and availability of service needed by the criminal justice community. | Current | CJIS/CSO | CJIS/CSO | CJIS/CSO |
| | | " | a. Ensure appropriate use, enforce system discipline, and ensure CJIS Division operating procedures are followed by all users of the respective services and information. | Current | CJIS/CSO | CJIS/CSO | CJIS/CSO |
| | | " | b. Ensure state/federal agency compliance with policies approved by the APB and adopted by the FBI. | Current | CJIS/CSO | CJIS/CSO | CJIS/CSO |
| | | " | c. Ensure the appointment of the CSA ISO and determine the extent of authority to the CSA ISO. | Current | CJIS/CSO | CJIS/CSO | CJIS/CSO |
| | | " | d. Ensure the designation of a Terminal Agency Coordinator (TAC) within each agency with device access to CJIS systems. | Current | Agency | Agency | Agency |
| | | " | e. Ensure each agency having access to CJI has someone designated as the Local Agency Security Officer (LASO). | Current | Agency | Agency | Agency |
| | | " | f. Ensure the LASO receives enhanced security awareness training (ref. Section 5.2). | Current | CJIS/CSO | CJIS/CSO | CJIS/CSO |
| | | " | g. Approve access to FBI CJIS systems. | Current | CJIS/CSO | CJIS/CSO | CJIS/CSO |
| | | " | h. Assume ultimate responsibility for managing the security of CJIS systems within their state and/or agency. | Current | CJIS/CSO | CJIS/CSO | CJIS/CSO |
| | | " | i. Perform other related duties outlined by the user agreements with the FBI CJIS Division. | Current | CJIS/CSO | CJIS/CSO | CJIS/CSO |
| 3.2.3(3) | 3.2.3(3) | " | 3. Outsourcing of Criminal Justice Functions | Current | | | |
| | | " | a. Responsibility for the management of the approved security requirements shall remain with the CJA. | Current | Agency | Agency | Agency |
| | | " | b. Responsibility for the management control of network security shall remain with the CJA. | Current | Agency | Agency | Agency |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|----------------------------------------|----------------------------------------|-----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|----------|----------|
| | | | | | IaaS | PaaS | SaaS |
| 3.2.6 | 3.2.6 | Contracting Government Agency (CGA) | A CGA is a government agency, whether a CJA or a NCJA, that enters into an agreement with a private contractor subject to the CJIS Security Addendum. The CGA entering into an agreement with a contractor shall appoint an Agency Coordinator. | Current | Agency | Agency | Agency |
| 3.2.7 | 3.2.7 | Agency Coordinator (AC) | The AC shall be responsible for the supervision and integrity of the system, training and continuing education of employees and operators, scheduling of initial training and testing, and certification testing and all required reports by NCIC. | Current | Agency | Agency | Agency |
| | | " | The AC shall : | Current | | | |
| | | " | 1. Understand the communications, records capabilities, and needs of the Contractor which is accessing federal and state records through or because of its relationship with the CGA. | Current | Agency | Agency | Agency |
| | | " | 2. Participate in related meetings and provide input and comments for system improvement. | Current | Agency | Agency | Agency |
| | | " | 3. Receive information from the CGA (e.g., system updates) and disseminate it to appropriate Contractor employees. | Current | Agency | Agency | Agency |
| | | " | 4. Maintain and update manuals applicable to the effectuation of the agreement, and provide them to the Contractor. | Current | Agency | Agency | Agency |
| | | " | 5. Maintain up-to-date records of Contractor's employees who access the system, including name, date of birth, social security number, date fingerprint card(s) submitted, date security clearance issued, and date initially trained, tested, certified or recertified (if applicable). | Current | Agency | Agency | Agency |
| | | " | 6. Train or ensure the training of Contractor personnel. If Contractor personnel access NCIC, schedule the operators for testing or a certification exam with the CSA staff, or AC staff with permission from the CSA staff. Schedule new operators for the certification exam within six (6) months of assignment. Schedule certified operators for biennial re-certification testing within thirty (30) days prior to the expiration of certification. Schedule operators for other mandated class. | Current | Agency | Agency | Agency |
| | | " | 7. The AC will not permit an untrained/untested or non-certified Contractor employee to access CJI or systems supporting CJI where access to CJI can be gained. | Current | Agency | Agency | Agency |
| | | " | 8. Where appropriate, ensure compliance by the Contractor with NCIC validation requirements. | Current | Agency | Agency | Agency |
| | | " | 9. Provide completed applicant fingerprint cards on each Contractor employee who accesses the system to the CJA (or, where appropriate, CSA) for criminal background investigation prior to such employee accessing the system. | Current | Agency | Agency | Agency |
| | | " | 10. Any other responsibility for the AC promulgated by the FBI. | Current | Agency | Agency | Agency |
| 3.2.8 | 3.2.8 | CJIS System Agency Information Security Officer (CSA ISO) | The CSA ISO shall : | Current | | | |
| | | " | 1. Serve as the security point of contact (POC) to the FBI CJIS Division ISO. | Current | CJIS/CSO | CJIS/CSO | CJIS/CSO |
| | | " | 2. Document technical compliance with the CJIS Security Policy with the goal to assure the confidentiality, integrity, and availability of criminal justice information to the user community throughout the CSA's user community, to include the local level. | Current | CJIS/CSO | CJIS/CSO | CJIS/CSO |
| | | " | 3. Document and provide assistance for implementing the security-related controls for the Interface Agency and its users. | Current | CJIS/CSO | CJIS/CSO | CJIS/CSO |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|----------------------------------------|----------------------------------------|----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|----------|----------|
| | | | | | IaaS | PaaS | SaaS |
| 3.2.8 | 3.2.8 | CJIS System Agency Information Security Officer (CSA ISO) (continued) | 4. Establish a security incident response and reporting procedure to discover, investigate, document, and report to the CSA, the affected criminal justice agency, and the FBI CJIS Division ISO major incidents that significantly endanger the security or integrity of CJI. | Current | CJIS/CSO | CJIS/CSO | CJIS/CSO |
| 3.2.9 | 3.2.9 | Local Agency Security Officer (LASO) | Each LASO shall : | Current | | | |
| | | " | 1. Identify who is using the CSA approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same. | Current | Agency | Agency | Agency |
| | | " | 2. Identify and document how the equipment is connected to the state system. | Current | Agency | Agency | Agency |
| | | " | 3. Ensure that personnel security screening procedures are being followed as stated in this policy. | Current | Agency | Agency | Agency |
| | | " | 4. Ensure the approved and appropriate security measures are in place and working as expected. | Current | Agency | Agency | Agency |
| | | " | 5. Support policy compliance and ensure CSA ISO is promptly informed of security incidents. | Current | Agency | Agency | Agency |
| 3.2.10 | 3.2.10 | FBI CJIS Division Information Security Officer (FBI CJIS ISO) | The FBI CJIS ISO shall : | Current | | | |
| | | " | 1. Maintain the CJIS Security Policy. | Current | CJIS/CSO | CJIS/CSO | CJIS/CSO |
| | | " | 2. Disseminate the FBI Director approved CJIS Security Policy. | Current | CJIS/CSO | CJIS/CSO | CJIS/CSO |
| | | " | 3. Serve as a liaison with the CSA's ISO and with other personnel across the CJIS community and in this regard provide technical guidance as to the intent and implementation of operational and technical policy issues. | Current | CJIS/CSO | CJIS/CSO | CJIS/CSO |
| | | " | 4. Serve as a point-of-contact (POC) for computer incident notification and distribution of security alerts to the CSOs and ISOs. | Current | CJIS/CSO | CJIS/CSO | CJIS/CSO |
| | | " | 5. Assist with developing audit compliance guidelines as well as identifying and reconciling security-related issues. | Current | CJIS/CSO | CJIS/CSO | CJIS/CSO |
| | | " | 6. Develop and participate in information security training programs for the CSOs and ISOs, and provide a means by which to acquire feedback to measure the effectiveness and success of such training. | Current | CJIS/CSO | CJIS/CSO | CJIS/CSO |
| | | " | 7. Maintain a security policy resource center (SPRC) on FBI.gov and keep the CSOs and ISOs updated on pertinent information. | Current | CJIS/CSO | CJIS/CSO | CJIS/CSO |
| 3.2.12 | 3.2.12 | Compact Officer | Pursuant to the National Crime Prevention and Privacy Compact, each party state shall appoint a Compact Officer... | Current | CJIS/CSO | CJIS/CSO | CJIS/CSO |
| | | | ...Compact Officer who shall ensure that Compact provisions and rules, procedures, and standards established by the Compact Council are complied with in their respective state. | Current | CJIS/CSO | CJIS/CSO | CJIS/CSO |
| 4.2.1 | 4.2.1 | Proper Access, Use, and Dissemination of CHRI | The III shall be accessed only for an authorized purpose. | Current | Agency | Agency | Agency |
| | | " | Further, CHRI shall only be used for an authorized purpose consistent with the purpose for which III was accessed. | Current | Agency | Agency | Agency |
| 4.2.2 | 4.2.2 | Proper Access, Use, and Dissemination of NCIC Restricted Files Information | Proper access to, use, and dissemination of data from restricted files shall be consistent with the access, use, and dissemination policies concerning the III described in Title 28, Part 20, CFR, and the NCIC Operating Manual. | Current | Agency | Agency | Agency |
| | | " | The restricted files, which shall be protected as CHRI, are as follows: | Current | | | |
| | | " | 1. Gang File | Current | Agency | Agency | Agency |
| | | " | 2. Threat Screening Center File | Current | Agency | Agency | Agency |
| | | " | 3. Supervised Release File | Current | Agency | Agency | Agency |
| | | " | 4. National Sex Offender Registry File | Current | Agency | Agency | Agency |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|----------------------------------------|----------------------------------------|----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|--------|--------|
| | | | | | IaaS | PaaS | SaaS |
| 4.2.2 | 4.2.2 | Proper Access, Use, and Dissemination of NCIC Restricted Files Information (continued) | 5. Historical Protection Order File of the NCIC | Current | Agency | Agency | Agency |
| | | " | 6. Identity Theft File | Current | Agency | Agency | Agency |
| | | " | 7. Protective Interest File | Current | Agency | Agency | Agency |
| | | " | 8. Person With Information [PWI] data in the Missing Person Files | Current | Agency | Agency | Agency |
| | | " | 9. Violent Person File | Current | Agency | Agency | Agency |
| | | " | 10. NICS Denied Transaction File | Current | Agency | Agency | Agency |
| 4.2.3.2 | 4.2.3.2 | For Other Authorized Purposes | Non-restricted files information shall not be disseminated commercially. | Current | Agency | Agency | Agency |
| | | " | Agencies shall not disseminate restricted files information for purposes other than law enforcement. | Current | Agency | Agency | Agency |
| 4.2.4 | 4.2.4 | Storage | When CHRI is stored, agencies shall establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of the information. | Current | Agency | Agency | Agency |
| | | " | These records shall be stored for extended periods only when they are key elements for the integrity and/or utility of case files and/or criminal record files. | Current | Agency | Agency | Agency |
| 4.2.5.1 | 4.2.5.1 | Justification | In addition to the use of purpose codes and logging information, all users shall provide a reason for all III inquiries whenever requested by NCIC System Managers, CSAs, local agency administrators, or their representatives. | Current | Agency | Agency | Agency |
| 4.3 | 4.3 | Personally Identifiable Information (PII) | PII shall be extracted from CJI for the purpose of official business only. | Current | Agency | Agency | Agency |
| | | " | Agencies shall develop policies, based on state and local privacy rules, to ensure appropriate controls are applied when handling PII extracted from CJI. | Current | Agency | Agency | Agency |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|-------------------------------------------------------------------|----------------------------------------|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|--------|--------|
| | | | | | IaaS | PaaS | SaaS |
| CJIS Security Policy Section 5-1: Information Exchange Agreements | | | | | | | |
| 5.1 | 5.1 | Policy Area 1: Information Exchange Agreements | The information shared through communication mediums shall be protected with appropriate security safeguards. | Current | Agency | Agency | Agency |
| 5.1.1 | 5.1.1 | Information Exchange | Before exchanging CJI, agencies shall put formal agreements in place that specify security controls. | Current | Agency | Agency | Agency |
| | | " | Information exchange agreements for agencies sharing CJI data that is sent to and/or received from the FBI CJIS shall specify the security controls and conditions described in this document. | Current | Agency | Agency | Agency |
| | | " | Information exchange agreements shall be supported by documentation committing both parties to the terms of information exchange. | Current | Agency | Agency | Agency |
| | | " | Law Enforcement and civil agencies shall have a local policy to validate a requestor of CJI as an authorized recipient before disseminating CJI. | Current | Agency | Agency | Agency |
| 5.1.1.1 | 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. | Current | Agency | Agency | Agency |
| | | " | Using the requirements in this policy as a starting point, the procedures shall apply to the handling, processing, storing, and communication of CJI. | Current | Agency | Agency | Agency |
| 5.1.1.2 | 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. | Current | Agency | Agency | Agency |
| | | " | This agreement shall include the standards and sanctions governing utilization of CJIS systems. | Current | Agency | Agency | Agency |
| | | " | 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. | Current | Agency | Agency | Agency |
| | | " | All user agreements with the FBI CJIS Division shall be coordinated with the CSA head. | Current | Agency | Agency | Agency |
| 5.1.1.3 | 5.1.1.3 | Criminal Justice Agency User Agreements | Any CJA receiving access to FBI CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA providing the access. | Current | Agency | Agency | Agency |
| | | " | 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. | Current | Agency | Agency | Agency |
| | | " | These agreements shall include: | Current | | | |
| | | " | 1. Audit. | Current | Agency | Agency | Agency |
| | | " | 2. Dissemination. | Current | Agency | Agency | Agency |
| | | " | 3. Hit confirmation. | Current | Agency | Agency | Agency |
| | | " | 4. Logging. | Current | Agency | Agency | Agency |
| | | " | 5. Quality Assurance (QA). | Current | Agency | Agency | Agency |
| | | " | 6. Screening (Pre-Employment). | Current | Agency | Agency | Agency |
| | | " | 7. Security. | Current | Agency | Agency | Agency |
| | | " | 8. Timeliness. | Current | Agency | Agency | Agency |
| | | " | 9. Training. | Current | Agency | Agency | Agency |
| | | " | 10. Use of the system. | Current | Agency | Agency | Agency |
| " | 11. Validation. | Current | Agency | Agency | Agency | | |
| 5.1.1.4 | 5.1.1.4 | Inter-Agency and Management Control Agreements | A NCJA (government) designated to perform criminal justice functions for a CJA shall be eligible for access to the CJI. | Current | Agency | Agency | Agency |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|----------------------------------------|----------------------------------------|---------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|----------|----------|
| | | | | | IaaS | PaaS | SaaS |
| 5.1.1.4 | 5.1.1.4 | Inter-Agency and Management Control Agreements (continued) | Access shall be permitted when such designation is authorized pursuant to Executive Order, statute, regulation, or inter-agency agreement. | Current | Agency | Agency | Agency |
| | | " | 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. | Current | Agency | Agency | Agency |
| 5.1.1.5 | 5.1.1.5 | Private Contractor User Agreements and CJIS Security Addendum | Private contractors who perform criminal justice functions shall meet the same training and certification criteria required by governmental agencies performing a similar function, and... | Current | Both | Both | Both |
| | | " | ...and shall be subject to the same extent of audit review as are local user agencies. | Current | Both | Both | Both |
| | | " | All private contractors who perform criminal justice functions shall acknowledge, via signing of the Security Addendum Certification page, and abide by all aspects of the CJIS Security Addendum. | Current | Both | Both | Both |
| | | " | Modifications to the CJIS Security Addendum shall be enacted only by the FBI. | Current | CJIS/CSO | CJIS/CSO | CJIS/CSO |
| | | " | 1. Private contractors designated to perform criminal justice functions for a CJA shall be eligible for access to CJI. | Current | Agency | Agency | Agency |
| | | " | Access shall be permitted pursuant to an agreement which specifically identifies the agency's purpose and scope of providing services for the administration of criminal justice. | Current | Agency | Agency | Agency |
| | | " | 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). | Current | Agency | Agency | Agency |
| | | " | 2. Private contractors designated to perform criminal justice functions on behalf of a NCJA (government) shall be eligible for access to CJI. | Current | Agency | Agency | Agency |
| | | " | Access shall be permitted pursuant to an agreement which specifically identifies the agency's purpose and scope of providing services for the administration of criminal justice. | Current | Agency | Agency | Agency |
| | | " | 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). | Current | Agency | Agency | Agency |
| 5.1.1.6 | 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. | Current | Agency | Agency | Agency |
| | | " | Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. | Current | Agency | Agency | Agency |
| | | " | A NCJA (public) receiving access to FBI CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA/SIB providing the access. | Current | Agency | Agency | Agency |
| | | " | 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. | Current | Agency | Agency | Agency |
| | | " | Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. | Current | Agency | Agency | Agency |
| | | " | A NCJA (private) receiving access to FBI CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA, SIB, or authorized agency providing the access. | Current | Agency | Agency | Agency |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|----------------------------------------|----------------------------------------|----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|--------|--------|
| | | | | | IaaS | PaaS | SaaS |
| 5.1.1.6 | 5.1.1.6 | Agency User Agreements (continued) | All NCJAs accessing CJI shall be subject to all pertinent areas of the CJIS Security Policy (see appendix J for supplemental guidance). | Current | Agency | Agency | Agency |
| | | " | 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. | Current | Agency | Agency | Agency |
| 5.1.1.7 | 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. | Current | Agency | Agency | Agency |
| | | " | Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. | Current | Agency | Agency | Agency |
| | | " | All Channelers accessing CJI shall be subject to the terms and conditions described in the Compact Council Security and Management Control Outsourcing Standard. | Current | Agency | Agency | Agency |
| | | " | Each Channeler that directly accesses CJI shall also allow the FBI to conduct periodic penetration testing. | Current | Agency | Agency | Agency |
| | | " | 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... | Current | Agency | Agency | Agency |
| | | " | ...and shall be subject to the same extent of audit review as are local user agencies. | Current | Agency | Agency | Agency |
| 5.1.1.8 | 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. | Current | Agency | Agency | Agency |
| | | " | Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. | Current | Agency | Agency | Agency |
| | | " | All contractors accessing CJI shall be subject to the terms and conditions described in the Compact Council Outsourcing Standard for Non-Channelers. | Current | Agency | Agency | Agency |
| | | " | 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... | Current | Agency | Agency | Agency |
| | | " | ...and shall be subject to the same extent of audit review as are local user agencies. | Current | Agency | Agency | Agency |
| 5.1.2 | 5.1.2 | Monitoring, Review, and Delivery of Services | As specified in the inter-agency agreements, MCAs, and contractual agreements with private contractors, the services, reports and records provided by the service provider shall be regularly monitored and reviewed. | Current | Agency | Agency | Agency |
| | | " | The CJA, authorized agency, or FBI shall maintain sufficient overall control and visibility into all security aspects to include, but not limited to, identification of vulnerabilities and information security incident reporting/response. | Current | Agency | Agency | Agency |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|----------------------------------------------|----------------------------------------------|----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|-----------------------------------------|--------|--------|
| | | | | | IaaS | PaaS | SaaS |
| 5.1.2 | 5.1.2 | Monitoring, Review, and Delivery of Services (continued) | The incident reporting/response process used by the service provider shall conform to the incident reporting/response specifications provided in this policy. | Current | Agency | Agency | Agency |
| 5.1.2.1 | 5.1.2.1 | Managing Changes to Service Providers | Any changes to services provided by a service provider shall be managed by the CJA, authorized agency, or FBI. | Current | Agency | Agency | Agency |
| | | " | Evaluation of the risks to the agency shall be undertaken based on the criticality of the data, system, and the impact of the change. | Current | Agency | Agency | Agency |
| 5.1.3 | 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. | Current | Agency | Agency | Agency |
| 5.1.4 | 5.1.4 | Secondary Dissemination of Non- CHRI CJI | Dissemination shall conform to the local policy validating the requestor of the CJI as an employee 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. | Current | Agency | Agency | Agency |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|---------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|------|------|
| | | | | | IaaS | PaaS | SaaS |
| CJIS Security Policy Section 5-2: Awareness and Training (AT) | | | | | | | |
| 5.2: AT-1 | 5.2: AT-1 | Policy and Procedures | a. Develop, document, and disseminate to all personnel when their unescorted logical or physical access to any information system results in the ability, right, or privilege to view, modify, or make use of unencrypted CJI: | 10/1/2023 | Both | Both | Both |
| | | " | 1. Organization-level awareness and training policy that: | 10/1/2023 | Both | Both | Both |
| | | " | (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and | 10/1/2023 | Both | Both | Both |
| | | " | (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and | 10/1/2023 | Both | Both | Both |
| | | " | 2. Procedures to facilitate the implementation of the awareness and training policy and the associated awareness and training controls; | 10/1/2023 | Both | Both | Both |
| | | " | b. Designate organizational personnel with information security awareness and training responsibilities to manage the development, documentation, and dissemination of the awareness and training policy nd procedures; and | 10/1/2023 | Both | Both | Both |
| | | " | c. Review and update the current awareness and training: | 10/1/2023 | Both | Both | Both |
| | | " | 1. Policy annually and following changes in the information system operating environment, when security incidents occur, or when changes to the CJIS Security Policy are made; and | 10/1/2023 | Both | Both | Both |
| | | " | 2. Procedures annually and following changes in the information system operating environment, when security incidents occur, or when changes to the CJIS Security Policy are made. | 10/1/2023 | Both | Both | Both |
| 5.2: AT-2 | 5.2: AT-2 | Literacy Training and Awareness | a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors): | Current | Both | Both | Both |
| | | " | 1. As part of initial training for new users prior to accessing CJI and annually thereafter; and | Current | Both | Both | Both |
| | | " | 2. When required by system changes or within 30 days of any security event for individuals involved in the event; | Current | Both | Both | Both |
| | | " | b. Employ one or more of the following techniques to increase the security and privacy awareness of system users: | Current | Both | Both | Both |
| | | " | 1. Displaying posters | Current | | | |
| | | " | 2. Offering supplies inscribed with security and privacy reminders | Current | | | |
| | | " | 3. Displaying logon screen messages | Current | | | |
| | | " | 4. Generating email advisories or notices from organizational officials | Current | | | |
| | | " | 5. Conducting awareness events | Current | | | |
| | | " | c. Update literacy training and awareness content annually and following changes in the information system operating environment, when security incidents occur, or when changes are made in the CJIS Security Policy; and | Current | Both | Both | Both |
| " | d. Incorporate lessons learned from internal or external security incidents or breaches into literacy training and awareness techniques. | Current | Both | Both | Both | | |
| 5.2: AT-2 (2) | 5.2: AT-2 (2) | LITERACY TRAINING AND AWARENESS INSIDER THREAT | Provide literacy training on recognizing and reporting potential indicators of insider threat. | Current | Both | Both | Both |
| 5.2: AT-2 (3) | 5.2: AT-2 (3) | LITERACY TRAINING AND AWARENESS SOCIAL ENGINEERING AND MINING | Provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining. | Current | Both | Both | Both |
| 5.2: AT-3 | 5.2: AT-3 | ROLE-BASED TRAINING | a. Provide role-based security and privacy training to personnel with the following roles and responsibilities: | Current | Both | Both | Both |
| | | " | · All individuals with unescorted access to a physically secure location; | Current | Both | Both | Both |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|----------------------------------------|----------------------------------------|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|------|------|
| | | | | | IaaS | PaaS | SaaS |
| 5.2: AT-3 | 5.2: AT-3 | ROLE-BASED TRAINING (continued) | · General User: A user, but not a process, who is authorized to use an information system; | Current | Both | Both | Both |
| | | " | · Privileged User: A user that is authorized (and, therefore, trusted) to perform security-relevant functions that general users are not authorized to perform: | Current | Both | Both | Both |
| | | " | 1. Before authorizing access to the system, information, or performing assigned duties, and annually thereafter; and | Current | Both | Both | Both |
| | | " | 2. When required by system changes; | Current | Both | Both | Both |
| | | " | b. Update role-based training content annually and following audits of the CSA and local agencies ; changes in the information system operating environment; security incidents; or when changes are made to the CJIS Security Policy; | Current | Both | Both | Both |
| | | " | c. Incorporate lessons learned from internal or external security incidents or breaches into role-based training; | Current | Both | Both | Both |
| | | " | d. Incorporate the minimum following topics into the appropriate role-based training content: | Current | Both | Both | Both |
| | | " | 1. All individuals with unescorted access to a physically secure location: | Current | | | |
| | | " | a. Access, Use and Dissemination of Criminal History Record Information (CHRI), NCIC Restricted Files Information, and NCIC Non-Restricted Files Information Penalties | Current | Both | Both | Both |
| | | " | b. Reporting Security Events | Current | Both | Both | Both |
| | | " | c. Training | Current | Both | Both | Both |
| | | " | d. System Use Notification | Current | Both | Both | Both |
| | | " | e. Physical Access Authorizations | Current | Both | Both | Both |
| | | " | f. Physical Access Control | Current | Both | Both | Both |
| | | " | g. Monitoring Physical Access | Current | Both | Both | Both |
| | | " | h. Visitor Control | Current | Both | Both | Both |
| | | " | i. Personnel Sanctions | Current | Both | Both | Both |
| | | " | 2. General User: A user, but not a process, who is authorized to use an information system. In addition to AT-3 (d) (1) above, include the following topics: | Current | | | |
| | | " | a. Criminal Justice Information | Current | Both | Both | Both |
| | | " | b. Proper Access, Use, and Dissemination of NCIC Non-Restricted Files Information | Current | Both | Both | Both |
| | | " | c. Personally Identifiable Information | Current | Both | Both | Both |
| | | " | d. Information Handling | Current | Both | Both | Both |
| | | " | e. Media Storage | Current | Both | Both | Both |
| | | " | f. Media Access | Current | Both | Both | Both |
| | | " | g. Audit Monitoring, Analysis, and Reporting | Current | Both | Both | Both |
| | | " | h. Access Enforcement | Current | Both | Both | Both |
| | | " | i. Least Privilege | Current | Both | Both | Both |
| | | " | j. System Access Control | Current | Both | Both | Both |
| | | " | k. Access Control Criteria | Current | Both | Both | Both |
| | | " | l. System Use Notification | Current | Both | Both | Both |
| | | " | m. Session Lock | Current | Both | Both | Both |
| | | " | n. Personally Owned Information Systems | Current | Both | Both | Both |
| | | " | o. Password | Current | Both | Both | Both |
| | | " | p. Access Control for Display Medium | Current | Both | Both | Both |
| | | " | q. Encryption | Current | Both | Both | Both |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|----------------------------------------|----------------------------------------|----------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|------|------|
| | | | | | IaaS | PaaS | SaaS |
| 5.2: AT-3 | 5.2: AT-3 | ROLE-BASED TRAINING (continued) | r. Malicious Code Protection | Current | Both | Both | Both |
| | | " | s. Spam and Spyware Protection | Current | Both | Both | Both |
| | | " | t. Cellular Devices | Current | Both | Both | Both |
| | | " | u. Mobile Device Management | Current | Both | Both | Both |
| | | " | v. Wireless Device Risk Mitigations | Current | Both | Both | Both |
| | | " | w. Wireless Device Malicious Code Protection | Current | Both | Both | Both |
| | | " | x. Literacy Training and Awareness/Social Engineering and Mining | Current | Both | Both | Both |
| | | " | y. Identification and Authentication (Organizational Users) | Current | Both | Both | Both |
| | | " | z. Media Protection | Current | Both | Both | Both |
| | | " | 3. Privileged User: A user that is authorized (and, therefore, trusted) to perform security-relevant functions that general users are not authorized to perform. In addition to AT-3 (d) (1) and (2) above, include the following topics: | Current | | | |
| | | " | a. Access Control | Current | Both | Both | Both |
| | | " | b. System and Communications Protection and Information Integrity | Current | Both | Both | Both |
| | | " | c. Patch Management | Current | Both | Both | Both |
| | | " | d. Data backup and storage—centralized or decentralized approach | Current | Both | Both | Both |
| | | " | e. Most recent changes to the CJIS Security Policy | Current | Both | Both | Both |
| | | " | 4. Organizational Personnel with Security Responsibilities: Personnel with the responsibility to ensure the confidentiality, integrity, and availability of CJI and the implementation of technology in a manner compliant with the CJISSECPOL. In addition to AT-3 (d) (1), (2), and (3) above, include the following topics: | Current | | | |
| | | " | a. Local Agency Security Officer Role | Current | Both | Both | Both |
| | | " | b. Authorized Recipient Security Officer Role | 10/1/2023 | Both | Both | Both |
| | | " | c. Additional state/local/tribal/federal agency LASO roles and responsibilities | Current | Both | Both | Both |
| | | " | d. Summary of audit findings from previous state audits of local agencies | Current | Both | Both | Both |
| | | " | e. Findings from the last FBI CJIS Division audit | Current | Both | Both | Both |
| 5.2: AT-3 (5) | 5.2: AT-3 (5) | ROLE-BASED TRAINING PROCESSING PERSONALLY IDENTIFIABLE INFORMATION | Provide all personnel when their unescorted logical or physical access to any information system results in the ability, right, or privilege to view, modify, or make use of unencrypted CJI with initial and annual training in the employment and operation of personally identifiable information processing and transparency controls. | 10/1/2023 | Both | Both | Both |
| 5.2: AT-4 | 5.2: AT-4 | TRAINING RECORDS | a. Document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training; and | Current | Both | Both | Both |
| | | " | b. Retain individual training records for a minimum of three years. | Current | Both | Both | Both |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|----------------------------------------------------------|----------------------------------------|-----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|------|------|
| | | | | | IaaS | PaaS | SaaS |
| CJIS Security Policy Section 5-3: Incident Response (IR) | | | | | | | |
| 5.3 | IR-1 | POLICY AND PROCEDURES | a. Develop, document, and disseminate to all personnel when their unescorted logical or physical access to any information system results in the ability, right, or privilege to view, modify, or make use of unencrypted CJI: | Current | Both | Both | Both |
| 5.3 | | " | 1. Agency-level incident response policy that: | Current | Both | Both | Both |
| 5.3.2 | | " | (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and | Current | Both | Both | Both |
| 5.3.2 | | " | (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and | Current | Both | Both | Both |
| 5.3 | | " | 2. Procedures to facilitate the implementation of the incident response policy and the associated incident response controls; | Current | Both | Both | Both |
| 5.3 | | " | b. Designate an individual with security responsibilities to manage the development, documentation, and dissemination of the incident response policy and procedures; and | Current | Both | Both | Both |
| | | " | c. Review and update the current incident response: | 10/1/2024 | Both | Both | Both |
| | | " | 1. Policy annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI; and | 10/1/2024 | Both | Both | Both |
| | | " | 2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI. | 10/1/2024 | Both | Both | Both |
| | | | | | | | |
| 5.3.3 | IR-2 | INCIDENT RESPONSE TRAINING | a. Provide incident response training to system users consistent with assigned roles and responsibilities: | Current | Both | Both | Both |
| 5.3.3 | | " | 1. Prior to assuming an incident response role or responsibility or acquiring system access; | Current | Both | Both | Both |
| 5.3.3 | | " | 2. When required by system changes; and | Current | Both | Both | Both |
| 5.3.3 | | " | 3. Annually thereafter; and | Current | Both | Both | Both |
| | | " | b. Review and update incident response training content annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI. | 10/1/2024 | Both | Both | Both |
| | IR-2 (3) | (3) INCIDENT RESPONSE TRAINING / BREACH | Provide incident response training on how to identify and respond to a breach, including the organization’s process for reporting a breach. | 10/1/2024 | Both | Both | Both |
| | IR-3 | INCIDENT RESPONSE TESTING | Control: Test the effectiveness of the incident response capability for the system annually using the following tests: tabletop or walk-through exercises; simulations; or other agency-appropriate tests. | 10/1/2024 | Both | Both | Both |
| | IR-3 (2) | (2) INCIDENT RESPONSE TESTING / COORDINATION WITH RELATED PLANS | Coordinate incident response testing with organizational elements responsible for related plans. | 10/1/2024 | Both | Both | Both |
| | | | | | | | |
| 5.3.2.1 | IR-4 | INCIDENT HANDLING | a. Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery; | Current | Both | Both | Both |
| 5.3.2.1 | | " | b. Coordinate incident handling activities with contingency planning activities; | Current | Both | Both | Both |
| 5.3.2.1 | | " | c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly; and | Current | Both | Both | Both |
| 5.3.2.1 | | " | d. Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization. | Current | Both | Both | Both |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|----------------------------------------|----------------------------------------|---------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|------|------|
| | | | | | IaaS | PaaS | SaaS |
| 5.3.2.1 | IR-4 (1) | (1) INCIDENT HANDLING AUTOMATED INCIDENT HANDLING PROCESSES | Support the incident handling process using automated mechanisms (e.g., online incident management systems and tools that support the collection of live response data, full network packet capture, and forensic analysis. | Current | Both | Both | Both |
| 5.3.4 | IR-5 | INCIDENT MONITORING | Control: Track and document incidents. | Current | Both | Both | Both |
| 5.3.1 | IR-6 | INCIDENT REPORTING | a. Require personnel to report suspected incidents to the organizational incident response capability immediately but not to exceed one (1) hour after discovery; and | Current | Both | Both | Both |
| 5.3.1 | | " | b. Report incident information to organizational personnel with incident handling responsibilities, and if confirmed, notify the CSO, SIB Chief, or Interface Agency Official. | Current | Both | Both | Both |
| 5.3.1 | IR-6 (1) | (1) INCIDENT REPORTING AUTOMATED REPORTING | Report incidents using automated mechanisms. | Current | Both | Both | Both |
| | IR-6 (3) | (3) INCIDENT REPORTING SUPPLY CHAIN COORDINATION | Provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident. | 10/1/2024 | Both | Both | Both |
| 5.3.1.1.2 | IR-7 | INCIDENT RESPONSE ASSISTANCE | Control: Provide an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the system for the handling and reporting of incidents. | Current | Both | Both | Both |
| | IR-7 (1) | (1) INCIDENT RESPONSE ASSISTANCE AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION AND SUPPORT | Increase the availability of incident response information and support using automated mechanisms described in the discussion. | 10/1/2024 | Both | Both | Both |
| 5.3 | IR-8 | INCIDENT RESPONSE PLAN | a. Develop an incident response plan that: | Current | Both | Both | Both |
| 5.3 | | " | 1. Provides the organization with a roadmap for implementing its incident response capability; | Current | Both | Both | Both |
| 5.3 | | " | 2. Describes the structure and organization of the incident response capability; | Current | Both | Both | Both |
| 5.3 | | " | 3. Provides a high-level approach for how the incident response capability fits into the overall organization; | Current | Both | Both | Both |
| 5.3 | | " | 4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; | Current | Both | Both | Both |
| 5.3 | | " | 5. Defines reportable incidents; | Current | Both | Both | Both |
| 5.3 | | " | 6. Provides metrics for measuring the incident response capability within the organization; | Current | Both | Both | Both |
| 5.3 | | " | 7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; | Current | Both | Both | Both |
| 5.3 | | " | 8. Addresses the sharing of incident information; | Current | Both | Both | Both |
| 5.3 | | " | 9. Is reviewed and approved by the organization's/agency's executive leadership annually; and | Current | Both | Both | Both |
| 5.3 | | " | 10. Explicitly designates responsibility for incident response to organizational personnel with incident reporting responsibilities and CSO or CJIS WAN Official. | Current | Both | Both | Both |
| 5.3 | | " | b. Distribute copies of the incident response plan to organizational personnel with incident handling responsibilities; | Current | Both | Both | Both |
| 5.3 | | " | c. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing; | Current | Both | Both | Both |
| 5.3 | | " | d. Communicate incident response plan changes to organizational personnel with incident handling responsibilities; and | Current | Both | Both | Both |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|----------------------------------------------|----------------------------------------------|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|-----------------------------------------|------|------|
| | | | | | IaaS | PaaS | SaaS |
| 5.3 | IR-8 | INCIDENT RESPONSE PLAN (continued) | e. Protect the incident response plan from unauthorized disclosure and modification. | Current | Both | Both | Both |
| | IR-8 (1) | (1) INCIDENT RESPONSE PLAN BREACHES | Include the following in the Incident Response Plan for breaches involving personally identifiable information: | 10/1/2024 | Both | Both | Both |
| | | " | (a) A process to determine if notice to individuals or other organizations, including oversight organizations, is needed; | 10/1/2024 | Both | Both | Both |
| | | " | (b) An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms; and | 10/1/2024 | Both | Both | Both |
| | | " | (c) Identification of applicable privacy requirements. | 10/1/2024 | Both | Both | Both |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|------------------------------------------------------------|----------------------------------------|----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|------------------|------------------|
| | | | | | IaaS | PaaS | SaaS |
| CJIS Security Policy Section 5-4: Audit and Accountability | | | | | | | |
| 5.4 | 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. | Current | Both | Both | Service Provider |
| | | " | Agencies shall carefully assess the inventory of components that compose their information systems to determine which security controls are applicable to the various components. | Current | Both | Service Provider | Service Provider |
| 5.4.1 | 5.4.1 | Auditable Events and Content (Information Systems) | The agency's information system shall generate audit records for defined events. | Current | Both | Both | Service Provider |
| | | " | The agency shall specify which information system components carry out auditing activities. | Current | Both | Both | Service Provider |
| | | " | 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. | Current | Both | Both | Service Provider |
| | | " | The agency shall periodically review and update the list of agency-defined auditable events. | Current | Both | Both | Service Provider |
| | | " | In the event an agency does not use an automated system, manual recording of activities shall still take place. | Current | Both | Both | Service Provider |
| 5.4.1.1 | 5.4.1.1 | Events | The following events shall be logged: | Current | | | |
| | | " | 1. Successful and unsuccessful system log-on attempts. | Current | Both | Both | Service Provider |
| | | " | 2. Successful and unsuccessful attempts to access, create, write, delete or change permission on a user account, file, directory or other system resource. | Current | Both | Both | Service Provider |
| | | " | 3. Successful and unsuccessful attempts to change account passwords. | Current | Both | Both | Service Provider |
| | | " | 4. Successful and unsuccessful actions by privileged accounts. | Current | Both | Both | Service Provider |
| | | " | 5. Successful and unsuccessful attempts for users to access, modify, or destroy the audit log file. | Current | Both | Both | Service Provider |
| 5.4.1.1.1 | 5.4.1.1.1 | Content | The following content shall be included with every audited event: | Current | | | |
| | | " | 1. Date and time of the event. | Current | Both | Both | Service Provider |
| | | " | 2.The component of the information system (e.g., software component, hardware component) where the event occurred. | Current | Both | Both | Service Provider |
| | | " | 3. Type of event. | Current | Both | Both | Service Provider |
| | | " | 4. User/subject identity. | Current | Both | Both | Service Provider |
| | | " | 5. Outcome (success or failure) of the event. | Current | Both | Both | Service Provider |
| 5.4.2 | 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. | Current | Both | Both | Both |
| 5.4.3 | 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. | Current | Both | Both | Both |
| | | " | Audit review/analysis shall be conducted at a minimum once a week. | Current | Both | Both | Both |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|----------------------------------------|----------------------------------------|-------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|--------|------------------|
| | | | | | IaaS | PaaS | SaaS |
| 5.4.3 | 5.4.3 | Audit Monitoring, Analysis, and Reporting (continued) | 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. | Current | Both | Both | Both |
| 5.4.4 | 5.4.4 | Time Stamps | The agency's information system shall provide time stamps for use in audit record generation. | Current | Both | Both | Service Provider |
| | | " | The time stamps shall include the date and time values generated by the internal system clocks in the audit records. | Current | Both | Both | Service Provider |
| | | " | The agency shall synchronize internal information system clocks on an annual basis. | Current | Both | Both | Service Provider |
| 5.4.5 | 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. | Current | Both | Both | Service Provider |
| 5.4.6 | 5.4.6 | Audit Record Retention | The agency shall retain audit records for at least one (1) year. | Current | Both | Both | Service Provider |
| | | " | 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. | Current | Both | Both | Service Provider |
| 5.4.7 | 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. | Current | Both | Both | Service Provider |
| | | " | The III portion of the log shall clearly identify both the operator and the authorized receiving agency. | Current | Agency | Agency | Agency |
| | | " | III logs shall also clearly identify the requester and the secondary recipient. | Current | Agency | Agency | Agency |
| | | " | 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. | Current | Agency | Agency | Agency |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|-------------------------------------------------------|----------------------------------------------|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|-----------------------------------------|------|------|
| | | | | | IaaS | PaaS | SaaS |
| CJIS Security Policy Section 5-5: Access Control (AC) | | | | | | | |
| | AC-1 | POLICY AND PROCEDURES | a. Develop, document, and disseminate to: organizational personnel with access control responsibilities | 10/1/2024 | Agency | Both | Both |
| | | " | 1. Agency-level access control policy that: | 10/1/2024 | Agency | Both | Both |
| | | " | (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and | 10/1/2024 | Agency | Both | Both |
| | | " | (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and | 10/1/2024 | Agency | Both | Both |
| | | " | 2. Procedures to facilitate the implementation of the access control policy and the associated access controls; | 10/1/2024 | Agency | Both | Both |
| | | " | b. Designate an individual with security responsibilities to manage the development, documentation, and dissemination of the access control policy and procedures; and | 10/1/2024 | Agency | Both | Both |
| | | " | c. Review and update the current access control: | 10/1/2024 | Agency | Both | Both |
| | | " | 1. Policy annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI; and | 10/1/2024 | Agency | Both | Both |
| | | " | 2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI. | 10/1/2024 | Agency | Both | Both |
| 5.5.1 | AC-2 | ACCOUNT MANAGEMENT | a. Define and document the types of accounts allowed and specifically prohibited for use within the system; | Current | Agency | Both | Both |
| 5.5.1 | | " | b. Assign account managers; | Current | Agency | Both | Both |
| 5.5.1 | | " | c. Require conditions for group and role membership; | Current | Agency | Both | Both |
| 5.5.1 | | " | d. Specify: | Current | Agency | Both | Both |
| 5.5.1 | | " | 1. Authorized users of the system; | Current | Agency | Both | Both |
| 5.5.1 | | " | 2. Group and role membership; and | Current | Agency | Both | Both |
| | | " | 3. Access authorizations (i.e., privileges) and attributes listed for each account; | 10/1/2024 | Agency | Both | Both |
| | | " | Attribute Name | 10/1/2024 | Agency | Both | Both |
| | | " | Email Address Text | 10/1/2024 | Agency | Both | Both |
| | | " | Employer Name | 10/1/2024 | Agency | Both | Both |
| | | " | Federation Id | 10/1/2024 | Agency | Both | Both |
| | | " | Given Name | 10/1/2024 | Agency | Both | Both |
| | | " | Identity Provider Id | 10/1/2024 | Agency | Both | Both |
| | | " | Sur Name | 10/1/2024 | Agency | Both | Both |
| | | " | Telephone Number | 10/1/2024 | Agency | Both | Both |
| | | " | Identity Provider Id | 10/1/2024 | Agency | Both | Both |
| | | " | Unique Subject Id | 10/1/2024 | Agency | Both | Both |
| | | " | Counter Terrorism Data Self Search Home Privilege Indicator | 10/1/2024 | Agency | Both | Both |
| | | " | Criminal History Data Self Search Home Privilege Indicator | 10/1/2024 | Agency | Both | Both |
| | | " | Criminal Intelligence Data Self Search Home Privilege Indicator | 10/1/2024 | Agency | Both | Both |
| | | " | Criminal Investigative Data Self Search Home Privilege Indicator | 10/1/2024 | Agency | Both | Both |
| | | " | Display Name | 10/1/2024 | Agency | Both | Both |
| | | " | Government Data Self Search Home Privilege Indicator | 10/1/2024 | Agency | Both | Both |
| | | " | Local Id | 10/1/2024 | Agency | Both | Both |
| | | " | NCIC Certification Indicator | 10/1/2024 | Agency | Both | Both |
| " | | NDEX Privilege Indicator | 10/1/2024 | Agency | Both | Both | |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|----------------------------------------|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|------|------|
| | | | | | IaaS | PaaS | SaaS |
| | AC-2 | ACCOUNT MANAGEMENT (continued) | PCII Certification Indicator | 10/1/2024 | Agency | Both | Both |
| | | " | 28 CFR Certification Indicator | 10/1/2024 | Agency | Both | Both |
| | | " | Employer ORI | 10/1/2024 | Agency | Both | Both |
| | | " | Employer Organization General Category Code | 10/1/2024 | Agency | Both | Both |
| | | " | Employer State Code | 10/1/2024 | Agency | Both | Both |
| | | " | Public Safety Officer Indicator | 10/1/2024 | Agency | Both | Both |
| | | " | Sworn Law Enforcement Officer Indicator | 10/1/2024 | Agency | Both | Both |
| | | " | Authenticator Assurance Level | 10/1/2024 | Agency | Both | Both |
| | | " | Federation Assurance Level | 10/1/2024 | Agency | Both | Both |
| | | " | Identity Assurance Level | 10/1/2024 | Agency | Both | Both |
| | | " | Intelligence Analyst Indicator | 10/1/2024 | Agency | Both | Both |
| 5.5.1 | | " | e. Require approvals by organizational personnel with account management responsibilities for requests to create accounts; | Current | Agency | Both | Both |
| 5.5.1 | | " | f. Create, enable, modify, disable, and remove accounts in accordance with agency policy; | Current | Agency | Both | Both |
| 5.5.1 | | " | g. Monitor the use of accounts; | Current | Agency | Both | Both |
| | | " | h. Notify account managers and system/network administrators within: | 10/1/2024 | Agency | Both | Both |
| | | " | 1. One day when accounts are no longer required; | 10/1/2024 | Agency | Both | Both |
| | | " | 2. One day when users are terminated or transferred; and | 10/1/2024 | Agency | Both | Both |
| | | " | 3. One day when system usage or need-to-know changes for an individual; | 10/1/2024 | Agency | Both | Both |
| 5.5.2.3 | | " | i. Authorize access to the system based on: | Current | Agency | Both | Both |
| 5.5.2.3 | | " | 1. A valid access authorization; | Current | Agency | Both | Both |
| 5.5.2.3 | " | 2. Intended system usage; and | Current | Agency | Both | Both | |
| | " | 3. Attributes as listed in AC-2(d)(3); | 10/1/2024 | Agency | Both | Both | |
| 5.5.1 | " | j. Review accounts for compliance with account management requirements at least annually; | Current | Agency | Both | Both | |
| 5.5.1 | " | k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and | Current | Agency | Both | Both | |
| 5.5.1 | " | l. Align account management processes with personnel termination and transfer processes. | Current | Agency | Both | Both | |
| | AC-2(1) | (1) ACCOUNT MANAGEMENT AUTOMATED SYSTEM ACCOUNT MANAGEMENT | Support the management of system accounts using automated mechanisms including email, phone, and text notifications. | 10/1/2024 | Agency | Both | Both |
| | AC-2(2) | (2) ACCOUNT MANAGEMENT AUTOMATED TEMPORARY AND EMERGENCY ACCOUNT MANAGEMENT | Automatically remove temporary and emergency accounts within 72 hours. | 10/1/2024 | Agency | Both | Both |
| | AC-2(3) | (3) ACCOUNT MANAGEMENT DISABLE ACCOUNTS | Disable accounts within one (1) week when the accounts: | 10/1/2024 | Agency | Both | Both |
| | | " | (a) Have expired; | 10/1/2024 | Agency | Both | Both |
| | | " | (b) Are no longer associated with a user or individual; | 10/1/2024 | Agency | Both | Both |
| | | " | (c) Are in violation of organizational policy; or | 10/1/2024 | Agency | Both | Both |
| | " | (d) Have been inactive for 90 calendar days. | 10/1/2024 | Agency | Both | Both | |
| | | | | | | | |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|----------------------------------------|----------------------------------------|-----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|------|------|
| | | | | | IaaS | PaaS | SaaS |
| 5.5.1 | AC-2(4) | (4) ACCOUNT MANAGEMENT AUTOMATED AUDIT ACTIONS | Automatically audit account creation, modification, enabling, disabling, and removal actions. | Current | Agency | Both | Both |
| | AC-2(5) | (5) ACCOUNT MANAGEMENT INACTIVITY LOGOUT | Require that users log out when a work period has been completed. | 10/1/2024 | Agency | Both | Both |
| | AC-2(13) | (13) ACCOUNT MANAGEMENT DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS | Disable accounts of individuals within 30 minutes of discovery of direct threats to the confidentiality, integrity, or availability of CJI. | 10/1/2024 | Agency | Both | Both |
| 5.5.2 | AC-3 | ACCESS ENFORCEMENT | Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | Current | Agency | Both | Both |
| 5.5.2 | AC-3(14) | (14) ACCESS ENFORCEMENT INDIVIDUAL ACCESS | Provide automated or manual processes to enable individuals to have access to elements of their personally identifiable information. | Current | Agency | Both | Both |
| 5.10.1 | AC-4 | INFORMATION FLOW ENFORCEMENT | Enforce approved authorizations for controlling the flow of information within the system and between connected systems by preventing CJI from being transmitted unencrypted across the public network, blocking outside traffic that claims to be from within the agency, and not passing any web requests to the public network that are not from agency controlled or internal boundary protection devices (e.g., proxies, gateways, firewalls, or routers). | Current | Agency | Both | Both |
| 5.5.2.1 | AC-5 | SEPARATION OF DUTIES | a. Identify and document separation of duties based on specific duties, operations, or information systems, as necessary, to mitigate risk to CJI; and | Current | Agency | Both | Both |
| 5.5.2.1 | | " | b. Define system access authorizations to support separation of duties. | Current | Agency | Both | Both |
| 5.5.2.1 | AC-6 | LEAST PRIVILEGE | Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks. | Current | Agency | Both | Both |
| 5.5.2.1 | AC-6(1) | (1) LEAST PRIVILEGE AUTHORIZE ACCESS TO SECURITY FUNCTIONS | Authorize access for personnel including, security administrators, system and network administrators, and other privileged users with access to system control, monitoring, or administration functions (e.g., system administrators, information security personnel, maintainers, system programmers, etc.) to: | Current | Agency | Both | Both |
| 5.5.2.1 | | " | (a) Established system accounts, configured access authorizations (i.e., permissions, privileges), set events to be audited, set intrusion detection parameters, and other security functions; and | Current | Agency | Both | Both |
| 5.5.2.1 | | " | (b) Security-relevant information in hardware, software, and firmware. | Current | Agency | Both | Both |
| 5.5.2.1 | AC-6(2) | (2) LEAST PRIVILEGE NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS | Require that users of system accounts (or roles) with access to privileged security functions or security-relevant information (e.g., audit logs), use non-privileged accounts or roles, when accessing nonsecurity functions. | Current | Agency | Both | Both |
| 5.5.2.1 | AC-6(5) | (5) LEAST PRIVILEGE PRIVILEGED ACCOUNTS | Restrict privileged accounts on the system to privileged users. | Current | Agency | Both | Both |
| 5.5.2.1 | AC-6(7) | (7) LEAST PRIVILEGE REVIEW OF USER PRIVILEGES | a. Reviews annually the privileges assigned to non-privileged and privileged users to validate the need for such privileges; and | Current | Agency | Both | Both |
| 5.5.2.1 | | " | b. Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs. | Current | Agency | Both | Both |
| 5.5.2.1 | AC-6(9) | (9) LEAST PRIVILEGE LOG USE OF PRIVILEGED FUNCTIONS | Log the execution of privileged functions. | Current | Agency | Both | Both |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|----------------------------------------|----------------------------------------|------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|------|------|
| | | | | | IaaS | PaaS | SaaS |
| 5.5.2.1 | AC-6(10) | (10) LEAST PRIVILEGE PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS | Prevent non-privileged users from executing privileged functions. | Current | Agency | Both | Both |
| | AC-7 | UNSUCCESSFUL LOGON ATTEMPTS | a. Enforce a limit of five (5) consecutive invalid logon attempts by a user during a 15-minute time period; and | 10/1/2024 | Agency | Both | Both |
| 5.5.3 | | " | b. Automatically lock the account or node until released by an administrator when the maximum number of unsuccessful attempts is exceeded. | Current | Agency | Both | Both |
| 5.5.4 | AC-8 | SYSTEM USE NOTIFICATION | a. Display a system use notification message to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that: | Current | Agency | Both | Both |
| 5.5.4 | | " | 1. Users are accessing a restricted information system; | Current | Agency | Both | Both |
| 5.5.4 | | " | 2. System usage may be monitored, recorded, and subject to audit; | Current | Agency | Both | Both |
| 5.5.4 | | " | 3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and | Current | Agency | Both | Both |
| 5.5.4 | | " | 4. Use of the system indicates consent to monitoring and recording; | Current | Agency | Both | Both |
| 5.5.4 | | " | b. Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system; and | Current | Agency | Both | Both |
| 5.5.4 | | " | c. For publicly accessible systems: | Current | Agency | Both | Both |
| 5.5.4 | | " | 1. Display system use information consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines, before granting further access to the publicly accessible system; | Current | Agency | Both | Both |
| 5.5.4 | | " | 2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and | Current | Agency | Both | Both |
| 5.5.4 | | " | 3. Include a description of the authorized uses of the system. | Current | Agency | Both | Both |
| 5.5.5 | AC-11 | DEVICE LOCK | a. Prevent further access to the system by initiating a device lock after a maximum of 30 minutes of inactivity and requiring the user to initiate a device lock before leaving the system unattended. | Current | Agency | Both | Both |
| 5.5.5 | | " | NOTE: In the interest of safety, devices that are: (1) part of a criminal justice conveyance; or (2) used to perform dispatch functions and located within a physically secure location; or (3) terminals designated solely for the purpose of receiving alert notifications (i.e., receive only terminals or ROT) used within physically secure location facilities that remain staffed when in operation, are exempt from this requirement. | Current | Agency | Both | Both |
| 5.5.5 | | " | b. Retain the device lock until the user reestablishes access using established identification and authentication procedures. | Current | Agency | Both | Both |
| 5.5.5 | AC-11(1) | (1) DEVICE LOCK PATTERN-HIDING DISPLAYS | Conceal, via the device lock, information previously visible on the display with a publicly viewable image. | Current | Agency | Both | Both |
| | AC-12 | SESSION TERMINATION | Automatically terminate a user session after a user has been logged out. | 10/1/2024 | Agency | Both | Both |
| | AC-14 | PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION | a. Identify any specific user actions that can be performed on the system without identification or authentication consistent with organizational mission and business functions; and | 10/1/2024 | Agency | Both | Both |
| | | " | b. Document and provide supporting rationale in the security plan for the system, user actions not requiring identification or authentication. | 10/1/2024 | Agency | Both | Both |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|----------------------------------------|----------------------------------------|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|------|------|
| | | | | | IaaS | PaaS | SaaS |
| 5.5.6 | AC-17 | REMOTE ACCESS | a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and | Current | Agency | Both | Both |
| 5.5.6 | | " | b. Authorize each type of remote access to the system prior to allowing such connections. | Current | Agency | Both | Both |
| 5.5.6 | AC-17(1) | (1) REMOTE ACCESS MONITORING AND CONTROL | Employ automated mechanisms to monitor and control remote access methods. | Current | Agency | Both | Both |
| 5.5.6 | AC-17(2) | (2) REMOTE ACCESS PROTECTION OF CONFIDENTIALITY AND INTEGRITY USING ENCRYPTION | Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions. | Current | Agency | Both | Both |
| 5.5.6 | AC-17(3) | (3) REMOTE ACCESS MANAGED ACCESS CONTROL POINTS | Route remote accesses through authorized and managed network access control points. | Current | Agency | Both | Both |
| 5.5.6 | AC-17(4) | (4) REMOTE ACCESS PRIVILEGED COMMANDS AND ACCESS | (a) Authorize the execution of privileged commands and access to security-relevant information via remote access only in a format that provides assessable evidence and for the following needs: compelling operational needs; and | Current | Agency | Both | Both |
| 5.5.6 | | " | (b) Document the rationale for remote access in the security plan for the system. | Current | Agency | Both | Both |
| 5.13 | AC-18 | WIRELESS ACCESS | a. Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access; and | Current | Agency | Both | Both |
| 5.13 | | " | b. Authorize each type of wireless access to the system prior to allowing such connections. | Current | Agency | Both | Both |
| 5.13 | AC-18(1) | (1) WIRELESS ACCESS AUTHENTICATION AND ENCRYPTION | Protect wireless access to the system using authentication of authorized users and agency-controlled devices, and encryption. | Current | Agency | Both | Both |
| 5.13 | AC-18(3) | (3) WIRELESS ACCESS DISABLE WIRELESS NETWORKING | Disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment. | Current | Agency | Both | Both |
| 5.13 | AC-19 | ACCESS CONTROL FOR MOBILE DEVICES | a. Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas; and | Current | Agency | Both | Both |
| 5.13 | | " | b. Authorize the connection of mobile devices to organizational systems. | Current | Agency | Both | Both |
| 5.13 | AC-19(5) | (5) ACCESS CONTROL FOR MOBILE DEVICES FULL DEVICE OR CONTAINER-BASED ENCRYPTION | Employ full-device encryption to protect the confidentiality and integrity of information on full- and limited-feature operating system mobile devices authorized to process, store, or transmit CJI. | Current | Agency | Both | Both |
| 5.5.6.1 | AC-20 | USE OF EXTERNAL SYSTEMS | a. Establish agency-level policies governing the use of external systems consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to: | Current | Agency | Both | Both |
| 5.5.6.1 | | " | 1. Access the system from external systems; and | Current | Agency | Both | Both |
| 5.5.6.1 | | " | 2. Process, store, or transmit organization-controlled information using external systems; or | Current | Agency | Both | Both |
| | | " | b. Prohibit the use of personally-owned information systems including mobile devices (i.e., bring your own device [BYOD]) and publicly accessible systems for accessing, processing, storing, or transmitting CJI. | 10/1/2024 | Agency | Both | Both |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|----------------------------------------|----------------------------------------|--------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|------|------|
| | | | | | IaaS | PaaS | SaaS |
| 5.5.6.1 | AC-20(1) | (1) USE OF EXTERNAL SYSTEMS LIMITS ON AUTHORIZED USE | <i>Permit authorized individuals to use an external system to access the system or to process, store, or transmit organization-controlled information only after:</i> | Current | Agency | Both | Both |
| 5.5.6.1 | | " | <i>(a) Verification of the implementation of controls on the external system as specified in the organization's security and privacy policies and security and privacy plans; or</i> | Current | Agency | Both | Both |
| 5.5.6.1 | | " | <i>(b) Retention of approved system connection or processing agreements with the organizational entity hosting the external system.</i> | Current | Agency | Both | Both |
| 5.5.6.1 | AC-20(2) | (2) USE OF EXTERNAL SYSTEMS PORTABLE STORAGE DEVICES — RESTRICTED USE | <i>Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems.</i> | Current | Agency | Both | Both |
| | AC-21 | INFORMATION SHARING | <i>a. Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions as defined in an executed information exchange agreement; and</i> | Current | Agency | Both | Both |
| | | " | <i>b. Employ attribute-based access control (see AC-2(d)(3)) or manual processes as defined in information exchange agreements to assist users in making information sharing and collaboration decisions.</i> | Current | Agency | Both | Both |
| | AC-22 | PUBLICLY ACCESSIBLE CONTENT | <i>a. Designate individuals authorized to make information publicly accessible;</i> | 10/1/2024 | Agency | Both | Both |
| | | " | <i>b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information;</i> | 10/1/2024 | Agency | Both | Both |
| | | " | <i>c. Review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included; and</i> | 10/1/2024 | Agency | Both | Both |
| | | " | <i>d. Review the content on the publicly accessible system for nonpublic information quarterly and remove such information, if discovered.</i> | 10/1/2024 | Agency | Both | Both |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|--------------------------------------------------------------------------|----------------------------------------|-------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|--------|--------|
| | | | | | IaaS | PaaS | SaaS |
| CJIS Security Policy Section 5-6: Identification and Authentication (IA) | | | | | | | |
| 5.6: IA-0 | 5.6: IA-0 | Use of Originating Agency Identifiers in Transactions and Information Exchanges | An FBI authorized originating agency identifier (ORI) shall be used in each transaction on CJIS systems in order to identify the sending agency and to ensure the proper level of access for each transaction. | Current | Agency | Agency | Agency |
| | | " | The original identifier between the requesting agency and the CSA/SIB/Channeler shall be the ORI, and other agency identifiers, such as user identification or personal identifier, an access device mnemonic, or the Internet Protocol (IP) address. | Current | Agency | Agency | Agency |
| | | " | Because the agency performing the transaction may not necessarily be the same as the agency requesting the transaction, the CSA/SIB/Channeler shall ensure that the ORI for each transaction can be traced, via audit trail, to the specific agency which is requesting the transaction. | Current | Agency | Agency | Agency |
| | | " | Agencies assigned a limited access ORI shall not use the full access ORI of another agency to conduct an inquiry transaction. | Current | Agency | Agency | Agency |
| 5.6: IA-1 | 5.6: IA-1 | Policy and Procedures | a. Develop, document, and disseminate to authorized personnel: | 10/1/2024 | Agency | Agency | Agency |
| | | " | 1. Agency/Entity identification and authentication policy that: | 10/1/2024 | Agency | Agency | Agency |
| | | " | (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and | 10/1/2024 | Agency | Agency | Agency |
| | | " | (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and | 10/1/2024 | Agency | Agency | Agency |
| | | " | 2. Procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls; | 10/1/2024 | Agency | Agency | Agency |
| | | " | b. Designate an individual with security responsibilities to manage the development, documentation, and dissemination of the identification and authentication policy and procedures; and | 10/1/2024 | Agency | Agency | Agency |
| | | " | c. Review and update the current identification and authentication: | 10/1/2024 | Agency | Agency | Agency |
| | | " | 1. Policy annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI; and | 10/1/2024 | Agency | Agency | Agency |
| | | " | 2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI. | 10/1/2024 | Agency | Agency | Agency |
| 5.6: IA-2 | 5.6: IA-2 | Identification and Authentication (Organizational Users) | Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users. | Current | Agency | Agency | Agency |
| 5.6: IA-2 (1) | 5.6: IA-2 (1) | Identification and Authentication (Organizational Users) Multi-Factor Authentication to Privileged Accounts | Implement multi-factor authentication for access to privileged accounts. | 10/1/2024 | Agency | Both | Both |
| 5.6: IA-2 (2) | 5.6: IA-2 (2) | Identification and Authentication (Organizational Users) Multi-Factor Authentication to Non-Privileged Accounts | Implement multi-factor authentication for access to non-privileged accounts. | 10/1/2024 | Agency | Both | Both |
| 5.6: IA-2 (8) | 5.6: IA-2 (8) | Identification and Authentication (Organizational Users) Access to Accounts - Replay Resistant | Implement replay-resistant authentication mechanisms for access to privileged and non-privileged accounts. | 10/1/2024 | Agency | Both | Both |
| 5.6: IA-2 (12) | 5.6: IA-2 (12) | Identification and Authentication (Organizational Users) Acceptance of PIV Credentials | Accept and electronically verify Personal Identity Verification-compliant credentials. | 10/1/2024 | Agency | Both | Both |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|----------------------------------------|----------------------------------------|----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|------|------|
| | | | | | IaaS | PaaS | SaaS |
| 5.6: IA-3 | 5.6: IA-3 | Device Identification and Authentication | Uniquely identify and authenticate agency devices before establishing all remote and network connections. In the instance of local connection, the device must be approved by the agency and the device must be identified and authenticated prior to connection to an agency asset. | 10/1/2024 | Agency | Both | Both |
| 5.6: IA-4 | 5.6: IA-4 | Identifier Management | Manage system identifiers by: | Current | Agency | Both | Both |
| | | " | a. Receiving authorization from organizational personnel with identifier management responsibilities to assign an individual, group, role, service, or device identifier; | Current | Agency | Both | Both |
| | | " | b. Selecting an identifier that identifies an individual, group, role, service, or device; | Current | Agency | Both | Both |
| | | " | c. Assigning the identifier to the intended individual, group, role, service, or device; and | Current | Agency | Both | Both |
| | | " | d. Preventing reuse of identifiers for one (1) year. | 10/1/2024 | Agency | Both | Both |
| 5.6: IA-4 (4) | 5.6: IA-4 (4) | Identifier Management Identify User Status | Manage individual identifiers by uniquely identifying each individual as agency or non-agency. | 10/1/2024 | Agency | Both | Both |
| 5.6: IA-5 | 5.6: IA-5 | Authenticator Management | Manage system authenticators by: | Current | Agency | Both | Both |
| | | " | a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator; | 10/1/2024 | Agency | Both | Both |
| | | " | b. Establishing initial authenticator content for any authenticators issued by the organization; | Current | Agency | Both | Both |
| | | " | c. Ensuring that authenticators have sufficient strength of mechanism for their intended use; | 10/1/2024 | Agency | Both | Both |
| | | " | d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators; | Current | Agency | Both | Both |
| | | " | e. Changing default authenticators prior to first use; | Current | Agency | Both | Both |
| | | " | f. Changing or refreshing authenticators annually or when there is evidence of authenticator compromise; | Current | Agency | Both | Both |
| | | " | g. Protecting authenticator content from unauthorized disclosure and modification; | Current | Agency | Both | Both |
| | | " | h. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and | 10/1/2024 | Agency | Both | Both |
| | | " | i. Changing authenticators for group or role accounts when membership to those accounts changes. | 10/1/2024 | Agency | Both | Both |
| | | " | j. All credential service providers (CSPs) authenticating claimants at Authenticator Assurance Level 2 (AAL2) SHALL be assessed on the following criteria: | | | | |
| | | " | (1) Authentication SHALL occur by the use of either a multi-factor authenticator or a combination of two single-factor authenticators. | 10/1/2024 | Agency | Both | Both |
| | | " | (2) If the multi-factor authentication process uses a combination of two single-factor authenticators, then it SHALL include a Memorized Secret authenticator and a possession-based authenticator. (NIST 800-63B, Section 4.2.1) | 10/1/2024 | Agency | Both | Both |
| | | " | (3) Cryptographic authenticators used at AAL2 SHALL use approved cryptography. | 10/1/2024 | Agency | Both | Both |
| | | " | (4) At least one authenticator used at AAL2 SHALL be replay resistant. | 10/1/2024 | Agency | Both | Both |
| | | " | (5) Communication between the claimant and verifier SHALL be via an authenticated protected channel. | 10/1/2024 | Agency | Both | Both |
| | | " | (6) Verifiers operated by government agencies at AAL2 SHALL be validated to meet the requirements of FIPS 140 Level 1. | 10/1/2024 | Agency | Both | Both |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|----------------------------------------|----------------------------------------|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|------|------|
| | | | | | IaaS | PaaS | SaaS |
| 5.6: IA-5 | 5.6: IA-5 | Authenticator Management (continued) | (7) Authenticators procured by government agencies SHALL be validated to meet the requirements of FIPS 140 Level 1. | 10/1/2024 | Agency | Both | Both |
| | | " | (8) If a device such as a smartphone is used in the authentication process, then the unlocking of that device (typically done using a PIN or biometric) SHALL NOT be considered one of the authentication factors. | 10/1/2024 | Agency | Both | Both |
| | | " | (9) If a biometric factor is used in authentication at AAL2, then the performance requirements stated in IA-5 m Biometric Requirements SHALL be met. | 10/1/2024 | Agency | Both | Both |
| | | " | (10) Reauthentication of the subscriber SHALL be repeated at least once per 12 hours during an extended usage session. | 10/1/2024 | Agency | Both | Both |
| | | " | (11) Reauthentication of the subscriber SHALL be repeated following any period of inactivity lasting 30 minutes or longer. | 10/1/2024 | Agency | Both | Both |
| | | " | (12) The CSP SHALL employ appropriately tailored security controls from the moderate baseline of security controls defined in the CJIS Security Policy. | 10/1/2024 | Agency | Both | Both |
| | | " | The CSP SHALL ensure that the minimum assurance-related controls for moderate-impact systems are satisfied. | 10/1/2024 | Agency | Both | Both |
| | | " | (13) The CSP SHALL comply with records retention policies in accordance with applicable laws and regulations. | 10/1/2024 | Agency | Both | Both |
| | | " | (14) If the CSP opts to retain records in the absence of any mandatory requirements, then the CSP SHALL conduct a risk management process, including assessments of privacy and security risks to determine how long records should be retained and SHALL inform subscribers of that retention policy. | 10/1/2024 | Agency | Both | Both |
| | | " | k. Privacy requirements that apply to all CSPs, verifiers, and RPs. | | | | |
| | | " | (1) The CSP SHALL employ appropriately tailored privacy controls from the CJIS Security Policy. | 10/1/2024 | Agency | Both | Both |
| | | " | (2) If the CSP processes attributes for purposes other than identity proofing, authentication, or attribute assertions (collectively "identity service"), related fraud mitigation, or to comply with law or legal process, then the CSP SHALL implement measures to maintain predictability and manageability commensurate with the associated privacy risk. | 10/1/2024 | Agency | Both | Both |
| | | " | l. General requirements applicable to AAL2 authentication process. | | | | |
| | | " | (1) CSPs SHALL provide subscriber instructions on how to appropriately protect a physical authenticator against theft or loss. | 10/1/2024 | Agency | Both | Both |
| | | " | (2) The CSP SHALL provide a mechanism to revoke or suspend the authenticator immediately upon notification from subscriber that loss or theft of the authenticator is suspected. | 10/1/2024 | Agency | Both | Both |
| | | " | (3) If required by the authenticator type descriptions in IA-5(1), then the verifier SHALL implement controls to protect against online guessing attacks. | 10/1/2024 | Agency | Both | Both |
| | | " | (4) If required by the authenticator type descriptions in IA-5(1) and the description of a given authenticator does not specify otherwise, then the verifier SHALL limit consecutive failed authentication attempts on a single account to no more than 100. | 10/1/2024 | Agency | Both | Both |
| | | " | (5) If signed attestations are used, then they SHALL be signed using a digital signature that provides at least the minimum security strength specified in the latest revision of 112 bits as of the date of this publication. | 10/1/2024 | Agency | Both | Both |
| | | " | (6) If the verifier and CSP are separate entities (as shown by the dotted line in Figure 8 Digital Identity Model), then communications between the verifier and CSP SHALL occur through a mutually-authenticated secure channel (such as a client-authenticated TLS connection). | 10/1/2024 | Agency | Both | Both |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|----------------------------------------|----------------------------------------|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|------|------|
| | | | | | IaaS | PaaS | SaaS |
| 5.6: IA-5 | 5.6: IA-5 | Authenticator Management (continued) | (7) If the CSP provides the subscriber with a means to report loss, theft, or damage to an authenticator using a backup or alternate authenticator, then that authenticator SHALL be either a memorized secret or a physical authenticator. | 10/1/2024 | Agency | Both | Both |
| | | " | (8) If the CSP chooses to verify an address of record (i.e., email, telephone, postal) and suspend authenticator(s) reported to have been compromised, then...The suspension SHALL be reversible if the subscriber successfully authenticates to the CSP using a valid (i.e., not suspended) authenticator and requests reactivation of an authenticator suspended in this manner. | 10/1/2024 | Agency | Both | Both |
| | | " | (9) If and when an authenticator expires, it SHALL NOT be usable for authentication. | 10/1/2024 | Agency | Both | Both |
| | | " | (10) The CSP SHALL have a documented process to require subscribers to surrender or report the loss of any physical authenticator containing attribute certificates signed by the CSP as soon as practical after expiration or receipt of a renewed authenticator. | 10/1/2024 | Agency | Both | Both |
| | | " | (11) CSPs SHALL revoke the binding of authenticators immediately upon notification when an online identity ceases to exist (e.g., subscriber's death, discovery of a fraudulent subscriber), when requested by the subscriber, or when the CSP determines that the subscriber no longer meets its eligibility requirements. | 10/1/2024 | Agency | Both | Both |
| | | " | (12) The CSP SHALL have a documented process to require subscribers to surrender or report the loss of any physical authenticator containing certified attributes signed by the CSP within five (5) days after revocation or termination takes place. | 10/1/2024 | Agency | Both | Both |
| | | " | m. Biometric Requirements | | | | |
| | | " | (1) Biometrics SHALL be used only as part of multi-factor authentication with a physical authenticator (something you have). | 10/1/2024 | Agency | Both | Both |
| | | " | (2) An authenticated protected channel between sensor (or an endpoint containing a sensor that resists sensor replacement) and verifier SHALL be established. | 10/1/2024 | Agency | Both | Both |
| | | " | (3) The sensor or endpoint SHALL be authenticated prior to capturing the biometric sample from the claimant. | 10/1/2024 | Agency | Both | Both |
| | | " | (4) The biometric system SHALL operate with an FMR [ISO/IEC 2382-37] of 1 in 1000 or better. This FMR SHALL be achieved under conditions of a conformant attack (i.e., zero-effort impostor attempt) as defined in [ISO/IEC 30107-1]. | 10/1/2024 | Agency | Both | Both |
| | | " | (5) The biometric system SHALL allow no more than 5 consecutive failed authentication attempts or 10 consecutive failed attempts if PAD demonstrating at least 90% resistance to presentation attacks is implemented. | 10/1/2024 | Agency | Both | Both |
| | | " | (6) Once the limit on authentication failures has been reached, the biometric authenticator SHALL either: | 10/1/2024 | Agency | Both | Both |
| | | " | i. Impose a delay of at least 30 seconds before the next attempt, increasing exponentially with each successive attempt, or | 10/1/2024 | Agency | Both | Both |
| | | " | ii. disable the biometric user authentication and offer another factor (e.g., a different biometric modality or a PIN/Passcode if it is not already a required factor) if such an alternative method is already available. | 10/1/2024 | Agency | Both | Both |
| | | " | (7) The verifier SHALL make a determination of sensor and endpoint performance, integrity, and authenticity. | 10/1/2024 | Agency | Both | Both |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|----------------------------------------|----------------------------------------|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|------|------|
| | | | | | IaaS | PaaS | SaaS |
| 5.6: IA-5 | 5.6: IA-5 | Authenticator Management (continued) | (8) If biometric comparison is performed centrally, then use of the biometric as an authentication factor SHALL be limited to one or more specific devices that are identified using approved cryptography. | 10/1/2024 | Agency | Both | Both |
| | | " | (9) If biometric comparison is performed centrally, then a separate key SHALL be used for identifying the device. | 10/1/2024 | Agency | Both | Both |
| | | " | (10) If biometric comparison is performed centrally, then biometric revocation, referred to as biometric template protection in ISO/IEC 24745, SHALL be implemented. | 10/1/2024 | Agency | Both | Both |
| | | " | (11) If biometric comparison is performed centrally, all transmission of biometrics SHALL be over the authenticated protected channel. | 10/1/2024 | Agency | Both | Both |
| | | " | (12) Biometric samples and any biometric data derived from the biometric sample such as a probe produced through signal processing SHALL be zeroized immediately after any training or research data has been derived | 10/1/2024 | Agency | Both | Both |
| | | " | n. Authenticator binding refers to the establishment of an association between a specific authenticator and a subscriber's account, enabling the authenticator to be used — possibly in conjunction with other authenticators — to authenticate for that account. | | | | |
| | | " | (1) Authenticators SHALL be bound to subscriber accounts by either issuance by the CSP as part of enrollment or associating a subscriber-provided authenticator that is acceptable to the CSP. | 10/1/2024 | Agency | Both | Both |
| | | " | (2) Throughout the digital identity lifecycle, CSPs SHALL maintain a record of all authenticators that are or have been associated with each identity. | 10/1/2024 | Agency | Both | Both |
| | | " | (3) The CSP or verifier SHALL maintain the information required for throttling authentication attempts. | 10/1/2024 | Agency | Both | Both |
| | | " | (4) The CSP SHALL also verify the type of user-provided authenticator so verifiers can determine compliance with requirements at each AAL. | 10/1/2024 | Agency | Both | Both |
| | | " | (5) The record created by the CSP SHALL contain the date and time the authenticator was bound to the account. | 10/1/2024 | Agency | Both | Both |
| | | " | (6) When any new authenticator is bound to a subscriber account, the CSP SHALL ensure that the binding protocol and the protocol for provisioning the associated key(s) are done at AAL2. | 10/1/2024 | Agency | Both | Both |
| | | " | (7) Protocols for key provisioning SHALL use authenticated protected channels or be performed in person to protect against man-in-the- middle attacks. | 10/1/2024 | Agency | Both | Both |
| | | " | (8) Binding of multi-factor authenticators SHALL require multi-factor authentication (or equivalent) at identity proofing. | 10/1/2024 | Agency | Both | Both |
| | | " | (9) At enrollment, the CSP SHALL bind at least one, and SHOULD bind at least two, physical (something you have) authenticators to the subscriber's online identity, in addition to a memorized secret or one or more biometrics. | 10/1/2024 | Agency | Both | Both |
| | | " | (10) At enrollment, authenticators at AAL2 and IAL2 SHALL be bound to the account. | 10/1/2024 | Agency | Both | Both |
| | | " | (11) If the subscriber is authenticated at AAL1, then the CSP SHALL NOT expose personal information, even if self-asserted, to the subscriber. | 10/1/2024 | Agency | Both | Both |
| | | " | (12) If enrollment and binding are being done remotely and cannot be completed in a single electronic transaction, then the applicant SHALL identify themselves in each new binding transaction by presenting a temporary secret which was either established during a prior transaction, or sent to the applicant's phone number, email address, or postal address of record. | 10/1/2024 | Agency | Both | Both |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|----------------------------------------|----------------------------------------|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|------|------|
| | | | | | IaaS | PaaS | SaaS |
| 5.6: IA-5 | 5.6: IA-5 | Authenticator Management (continued) | (13) If enrollment and binding are being done remotely and cannot be completed in a single electronic transaction, then long-term authenticator secrets are delivered to the applicant within a protected session. | 10/1/2024 | Agency | Both | Both |
| | | " | (14) If enrollment and binding are being done in person and cannot be completed in a single physical encounter, the applicant SHALL identify themselves in person by either using a secret as described in IA-5 n (12) above, or through use of a biometric that was recorded during a prior encounter. | 10/1/2024 | Agency | Both | Both |
| | | " | (15) If enrollment and binding are being done in person and cannot be completed in a single physical encounter, temporary secrets SHALL NOT be reused. | 10/1/2024 | Agency | Both | Both |
| | | " | (16) If enrollment and binding are being done in person and cannot be completed in a single physical encounter and the CSP issues long-term authenticator secrets during a physical transaction, they SHALL be loaded locally onto a physical device that is issued in person to the applicant or delivered in a manner that confirms the address of record. | 10/1/2024 | Agency | Both | Both |
| | | " | (17) Before adding a new authenticator to a subscriber's account, the CSP SHALL first require the subscriber to authenticate at AAL2 (or a higher AAL) at which the new authenticator will be used. | 10/1/2024 | Agency | Both | Both |
| | | " | (18) If the subscriber's account has only one authentication factor bound to it, the CSP SHALL require the subscriber to authenticate at AAL1 in order to bind an additional authenticator of a different authentication factor. | 10/1/2024 | Agency | Both | Both |
| | | " | (19) If a subscriber loses all authenticators of a factor necessary to complete multi-factor authentication and has been identity proofed at IAL2, that subscriber SHALL repeat the identity proofing process described in IA-12. | 10/1/2024 | Agency | Both | Both |
| | | " | (20) If a subscriber loses all authenticators of a factor necessary to complete multi-factor authentication and has been identity proofed at IAL2 or IAL3, the CSP SHALL require the claimant to authenticate using an authenticator of the remaining factor, if any, to confirm binding to the existing identity. | 10/1/2024 | Agency | Both | Both |
| | | " | (21) If the CSP opts to allow binding of a new memorized secret with the use of two physical authenticators, then it requires entry of a confirmation code sent to an address of record. | 10/1/2024 | Agency | Both | Both |
| | | " | (22) If the CSP opts to allow binding of a new memorized secret with the use of two physical authenticators, then the confirmation code SHALL consist of at least 6 random alphanumeric characters generated by an approved random bit generator [SP 800-90Ar1]. | 10/1/2024 | Agency | Both | Both |
| | | " | (23) If the CSP opts to allow binding of a new memorized secret with the use of two physical authenticators, then the confirmation code SHALL be valid for a maximum of 7 days but MAY be made valid up to 21 days via an exception process to accommodate addresses outside the direct reach of the U.S. Postal Service. Confirmation codes sent by means other than physical mail SHALL be valid for a maximum of 5 minutes. | 10/1/2024 | Agency | Both | Both |
| | | " | o. Session Management: The following requirements apply to applications where a session is maintained between the subscriber and relying party to allow multiple interactions without repeating the authentication event each time. | | | | |
| | | " | (1) Session Binding Requirements: A session occurs between the software that a subscriber is running — such as a browser, application, or operating system (i.e., the session subject) — and the RP or CSP that the subscriber is accessing (i.e., the session host). | 10/1/2024 | Agency | Both | Both |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|----------------------------------------|----------------------------------------|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|------|------|
| | | | | | IaaS | PaaS | SaaS |
| 5.6: IA-5 | 5.6: IA-5 | Authenticator Management (continued) | a. A session is maintained by a session secret which SHALL be shared between the subscriber's software and the service being accessed. | 10/1/2024 | Agency | Both | Both |
| | | " | b. The secret SHALL be presented directly by the subscriber's software or possession of the secret SHALL be proven using a cryptographic mechanism. | 10/1/2024 | Agency | Both | Both |
| | | " | c. The secret used for session binding SHALL be generated by the session host in direct response to an authentication event. | 10/1/2024 | Agency | Both | Both |
| | | " | d. A session SHALL NOT be considered at a higher AAL than the authentication event. | 10/1/2024 | Agency | Both | Both |
| | | " | e. Secrets used for session binding SHALL be generated by the session host during an interaction, typically immediately following authentication. | 10/1/2024 | Agency | Both | Both |
| | | " | f. Secrets used for session binding SHALL be generated by an approved random bit generator [SP 800-90Ar1]. | 10/1/2024 | Agency | Both | Both |
| | | " | g. Secrets used for session binding SHALL contain at least 64 bits of entropy. | 10/1/2024 | Agency | Both | Both |
| | | " | h. Secrets used for session binding SHALL be erased or invalidated by the session subject when the subscriber logs out. | 10/1/2024 | Agency | Both | Both |
| | | " | i. Secrets used for session binding SHALL be sent to and received from the device using an authenticated protected channel. | 10/1/2024 | Agency | Both | Both |
| | | " | j. Secrets used for session binding SHALL time out and not be accepted after the times specified in IA-5 j (13) as appropriate for the AAL. | 10/1/2024 | Agency | Both | Both |
| | | " | k. Secrets used for session binding SHALL NOT be available to insecure communications between the host and subscriber's endpoint. | 10/1/2024 | Agency | Both | Both |
| | | " | l. Authenticated sessions SHALL NOT fall back to an insecure transport, such as from https to http, following authentication. | 10/1/2024 | Agency | Both | Both |
| | | " | m. URLs or POST content SHALL contain a session identifier that SHALL be verified by the RP to ensure that actions taken outside the session do not affect the protected session. | 10/1/2024 | Agency | Both | Both |
| | | " | n. Browser cookies SHALL be tagged to be accessible only on secure (HTTPS) sessions. | 10/1/2024 | Agency | Both | Both |
| | | " | o. Browser cookies SHALL be accessible to the minimum practical set of hostnames and paths. | 10/1/2024 | Agency | Both | Both |
| | | " | p. Expiration of browser cookies SHALL NOT be depended upon to enforce session timeouts. | 10/1/2024 | Agency | Both | Both |
| | | " | q. The presence of an OAuth access token SHALL NOT be interpreted by the RP as presence of the subscriber, in the absence of other signals. | 10/1/2024 | Agency | Both | Both |
| | | " | (2) Reauthentication Requirements | | | | |
| | | " | a. Continuity of authenticated sessions SHALL be based upon the possession of a session secret issued by the verifier at the time of authentication and optionally refreshed during the session. | 10/1/2024 | Agency | Both | Both |
| | | " | b. Session secrets SHALL be non-persistent, i.e., they SHALL NOT be retained across a restart of the associated application or a reboot of the host device. | 10/1/2024 | Agency | Both | Both |
| | | " | c. Periodic reauthentication of sessions (at least every 12 hours per session) SHALL be performed to confirm the continued presence of the subscriber at an authenticated session. | 10/1/2024 | Agency | Both | Both |
| | | " | d. A session SHALL NOT be extended past the guidelines in IA-5 o (2) a – j based on presentation of the session secret alone. | 10/1/2024 | Agency | Both | Both |
| | | " | e. Prior to session expiration, the reauthentication time limit SHALL be extended by prompting the subscriber for the authentication factor(s) of a memorized secret or biometric. | 10/1/2024 | Agency | Both | Both |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|----------------------------------------|----------------------------------------|------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|------|------|
| | | | | | IaaS | PaaS | SaaS |
| 5.6: IA-5 | 5.6: IA-5 | Authenticator Management (continued) | f. If federated authentication is being used, then since the CSP and RP often employ separate session management technologies, there SHALL NOT be any assumption of correlation between these sessions. | 10/1/2024 | Agency | Both | Both |
| | | " | g. An RP requiring reauthentication through a federation protocol SHALL — if possible within the protocol — specify the maximum (see IA-5 j (10)) acceptable authentication age to the CSP. | 10/1/2024 | Agency | Both | Both |
| | | " | h. If federated authentication if being used and an RP has specific authentication age (see IA-5 j (10)) requirements that it has communicated to the CSP, then the CSP SHALL reauthenticate the subscriber if they have not been authenticated within that time period. | 10/1/2024 | Agency | Both | Both |
| | | " | i. If federated authentication is being used, the CSP SHALL communicate the authentication event time to the RP to allow the RP to decide if the assertion is sufficient for reauthentication and to determine the time for the next reauthentication event. | 10/1/2024 | Agency | Both | Both |
| 5.6: IA-5 (1) | 5.6: IA-5 (1) | Authenticator Management Authenticator Types | (a) Memorized Secret Authenticators and Verifiers: | | | | |
| | | " | (1) Maintain a list of commonly-used, expected, or compromised passwords and update the list quarterly and when organizational passwords are suspected to have been compromised directly or indirectly; | Current | Agency | Both | Both |
| | | " | (2) Require immediate selection of a new password upon account recovery; | 10/1/2024 | Agency | Both | Both |
| | | " | (3) Allow user selection of long passwords and passphrases, including spaces and all printable characters; | 10/1/2024 | Agency | Both | Both |
| | | " | (4) Employ automated tools to assist the user in selecting strong password authenticators; | 10/1/2024 | Agency | Both | Both |
| | | " | (5) Enforce the following composition and complexity rules: when agencies elect to follow basic password standards. | Current | Agency | Both | Both |
| | | " | (a) Not be a proper name. | Current | Agency | Both | Both |
| | | " | (b) Not be the same as the Userid. | Current | Agency | Both | Both |
| | | " | (c) Expire within a maximum of 90 calendar days. | Current | Agency | Both | Both |
| | | " | (d) Not be identical to the previous ten (10) passwords. | Current | Agency | Both | Both |
| | | " | (e) Not be displayed when entered. | Current | Agency | Both | Both |
| | | " | (6) If chosen by the subscriber, memorized secrets SHALL be at least 8 characters in length. | Current | Agency | Both | Both |
| | | " | (7) If chosen by the CSP or verifier using an approved random number generator, memorized secrets SHALL be at least 6 characters in length. | 10/1/2024 | Agency | Both | Both |
| | | " | (8) Truncation of the secret SHALL NOT be performed. | 10/1/2024 | Agency | Both | Both |
| | | " | (9) Memorized secret verifiers SHALL NOT permit the subscriber to store a “hint” that is accessible to an unauthenticated claimant. | Current | Agency | Both | Both |
| | | " | (10) Verifiers SHALL NOT prompt subscribers to use specific types of information (e.g., “What was the name of your first pet?”) when choosing memorized secrets. | Current | Agency | Both | Both |
| | | " | (11) When processing requests to establish and change memorized secrets, verifiers SHALL compare the prospective secrets against a list that contains values known to be commonly used, expected, or compromised. | Current | Agency | Both | Both |
| | | " | (12) If a chosen secret is found in the list, the CSP or verifier SHALL advise the subscriber that they need to select a different secret. | Current | Agency | Both | Both |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|----------------------------------------|----------------------------------------|------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|------|------|
| | | | | | IaaS | PaaS | SaaS |
| 5.6: IA-5 (1) | 5.6: IA-5 (1) | Authenticator Management Authenticator Types (continued) | (13) If a chosen secret is found in the list, the CSP or verifier SHALL provide the reason for rejection. | Current | Agency | Both | Both |
| | | " | (14) If a chosen secret is found in the list, the CSP or verifier SHALL require the subscriber to choose a different value. | Current | Agency | Both | Both |
| | | " | (15) Verifiers SHALL implement a rate-limiting mechanism that effectively limits failed authentication attempts that can be made on the subscriber's account to no more than five. | Current | Agency | Both | Both |
| | | " | (16) Verifiers SHALL force a change of memorized secret if there is evidence of compromise of the authenticator. | Current | Agency | Both | Both |
| | | " | (17) The verifier SHALL use approved encryption when requesting memorized secrets in order to provide resistance to eavesdropping and MitM attacks. | Current | Agency | Both | Both |
| | | " | (18) The verifier SHALL use an authenticated protected channel when requesting memorized secrets in order to provide resistance to eavesdropping and MitM attacks. | Current | Agency | Both | Both |
| | | " | (19) Verifiers SHALL store memorized secrets in a form that is resistant to offline attacks. | Current | Agency | Both | Both |
| | | " | (20) Memorized secrets SHALL be salted and hashed using a suitable one-way key derivation function. | Current | Agency | Both | Both |
| | | " | (21) The salt SHALL be at least 32 bits in length and be chosen arbitrarily to minimize salt value collisions among stored hashes. | Current | Agency | Both | Both |
| | | " | (22) Both the salt value and the resulting hash SHALL be stored for each subscriber using a memorized secret authenticator | Current | Agency | Both | Both |
| | | " | (23) If an additional iteration of a key derivation function using a salt value known only to the verifier is performed, then this secret salt value SHALL be generated with an approved random bit generator and of sufficient length. | 10/1/2024 | Agency | Both | Both |
| | | " | (24) If an additional iteration of a key derivation function using a salt value known only to the verifier is performed, then this secret salt value SHALL provide at least the minimum-security strength. | 10/1/2024 | Agency | Both | Both |
| | | " | (25) If an additional iteration of a key derivation function using a salt value known only to the verifier is performed, then this secret salt value SHALL be stored separately from the memorized secrets. | 10/1/2024 | Agency | Both | Both |
| | | " | (b) Look-Up Secret Authenticators and Verifiers | | | | |
| | | " | (1) CSPs creating look-up secret authenticators SHALL use an approved random bit generator to generate the list of secrets. | 10/1/2024 | Agency | Both | Both |
| | | " | (2) Look-up secrets SHALL have at least 20 bits of entropy. | 10/1/2024 | Agency | Both | Both |
| | | " | (3) If look-up secrets are distributed online, then they SHALL be distributed over a secure channel in accordance with the post-enrollment binding requirements in IA-5 n 17 through 25. | 10/1/2024 | Agency | Both | Both |
| | | " | (4) Verifiers of look-up secrets SHALL prompt the claimant for the next secret from their authenticator or for a specific (e.g., numbered) secret. | 10/1/2024 | Agency | Both | Both |
| | | " | (5) A given secret from an authenticator SHALL be used successfully only once. | 10/1/2024 | Agency | Both | Both |
| | | " | (6) If a look-up secret is derived from a grid (bingo) card, then each cell of the grid SHALL be used only once. | 10/1/2024 | Agency | Both | Both |
| | | " | (7) Verifiers SHALL store look-up secrets in a form that is resistant to offline attacks. | 10/1/2024 | Agency | Both | Both |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|----------------------------------------|----------------------------------------|------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|------|------|
| | | | | | IaaS | PaaS | SaaS |
| 5.6: IA-5 (1) | 5.6: IA-5 (1) | Authenticator Management Authenticator Types (continued) | (8) If look-up secrets have at least 112 bits of entropy, then they SHALL be hashed with an approved one-way function | 10/1/2024 | Agency | Both | Both |
| | | " | (9) If look-up secrets have less than 112 bits of entropy, then they SHALL be salted and hashed using a suitable one-way key derivation function. | 10/1/2024 | Agency | Both | Both |
| | | " | (10) If look-up secrets have less than 112 bits of entropy, then the salt SHALL be at least 32 bits in length and be chosen arbitrarily to minimize salt value collisions among stored hashes. | 10/1/2024 | Agency | Both | Both |
| | | " | (11) If look-up secrets have less than 112 bits of entropy, then both the salt value and the resulting hash SHALL be stored for each look-up secret | 10/1/2024 | Agency | Both | Both |
| | | " | (12) If look-up secrets that have less than 64 bits of entropy, then the verifier SHALL implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber's account. | 10/1/2024 | Agency | Both | Both |
| | | " | (13) The verifier SHALL use approved encryption when requesting look-up secrets in order to provide resistance to eavesdropping and MitM attacks. | 10/1/2024 | Agency | Both | Both |
| | | " | (14) The verifier SHALL use an authenticated protected channel when requesting look-up secrets in order to provide resistance to eavesdropping and MitM attacks. | 10/1/2024 | Agency | Both | Both |
| | | " | (c) Out-of-Band Authenticators and Verifiers | | | | |
| | | " | (1) The out-of-band authenticator SHALL establish a separate channel with the verifier in order to retrieve the out-of-band secret or authentication request. | 10/1/2024 | Agency | Both | Both |
| | | " | (2) Communication over the secondary channel SHALL be encrypted unless sent via the public switched telephone network (PSTN). | 10/1/2024 | Agency | Both | Both |
| | | " | (3) Methods that do not prove possession of a specific device, such as voice-over-IP (VOIP) or email, SHALL NOT be used for out-of-band authentication. | 10/1/2024 | Agency | Both | Both |
| | | " | (4) If PSTN is not being used for out-of-band communication, then the out-of-band authenticator SHALL uniquely authenticate itself by establishing an authenticated protected channel with the verifier. | 10/1/2024 | Agency | Both | Both |
| | | " | (5) If PSTN is not being used for out-of-band communication, then the out-of-band authenticator SHALL communicate with the verifier using approved cryptography. | 10/1/2024 | Agency | Both | Both |
| | | " | (6) If PSTN is not being used for out-of-band communication, then the key used to authenticate the out-of-band device SHALL be stored in suitably secure storage available to the authenticator application (e.g., keychain storage, TPM, TEE, secure element). | 10/1/2024 | Agency | Both | Both |
| | | " | (7) If the PSTN is used for out-of-band authentication and a secret is sent to the out-of-band device via the PSTN, then the out-of-band authenticator SHALL uniquely authenticate itself to a mobile telephone network using a SIM card or equivalent that uniquely identifies the device. | 10/1/2024 | Agency | Both | Both |
| | | " | (8) If the out-of-band authenticator sends an approval message over the secondary communication channel, it SHALL either accept transfer of a secret from the primary channel to be sent to the verifier via the secondary communications channel, or present a secret received via the secondary channel from the verifier and prompt the claimant to verify the consistency of that secret with the primary channel, prior to accepting a yes/no response from the claimant which it sends to the verifier. | 10/1/2024 | Agency | Both | Both |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|----------------------------------------|----------------------------------------|------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|------|------|
| | | | | | IaaS | PaaS | SaaS |
| 5.6: IA-5 (1) | 5.6: IA-5 (1) | Authenticator Management Authenticator Types (continued) | (9) The verifier SHALL NOT store the identifying key itself, but SHALL use a verification method (e.g., an approved hash function or proof of possession of the identifying key) to uniquely identify the authenticator. | 10/1/2024 | Agency | Both | Both |
| | | " | (10) Depending on the type of out-of-band authenticator, one of the following SHALL take place: transfer of a secret to the primary channel, transfer of a secret to the secondary channel, or verification of secrets by the claimant. | 10/1/2024 | Agency | Both | Both |
| | | " | (11) If the out-of-band authenticator operates by transferring the secret to the primary channel, then the verifier SHALL transmit a random secret to the out-of-band authenticator and then wait for the secret to be returned on the primary communication channel. | 10/1/2024 | Agency | Both | Both |
| | | " | (12) If the out-of-band authenticator operates by transferring the secret to the secondary channel, then the verifier SHALL display a random authentication secret to the claimant via the primary channel and then wait for the secret to be returned on the secondary channel from the claimant's out-of- band authenticator. | 10/1/2024 | Agency | Both | Both |
| | | " | (13) If the out-of-band authenticator operates by verification of secrets by the claimant, then the verifier SHALL display a random authentication secret to the claimant via the primary channel, send the same secret to the out-of-band authenticator via the secondary channel for presentation to the claimant, and then wait for an approval (or disapproval) message via the secondary channel. | 10/1/2024 | Agency | Both | Both |
| | | " | (14) The authentication SHALL be considered invalid if not completed within 10 minutes. | 10/1/2024 | Agency | Both | Both |
| | | " | (15) Verifiers SHALL accept a given authentication secret only once during the validity period. | 10/1/2024 | Agency | Both | Both |
| | | " | (16) The verifier SHALL generate random authentication secrets with at least 20 bits of entropy. | 10/1/2024 | Agency | Both | Both |
| | | " | (17) The verifier SHALL generate random authentication secrets using an approved random bit generator. | 10/1/2024 | Agency | Both | Both |
| | | " | (18) If the authentication secret has less than 64 bits of entropy, the verifier SHALL implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber's account as described in IA-5 I (3) through (4). | 10/1/2024 | Agency | Both | Both |
| | | " | (19) If out-of-band verification is to be made using the PSTN, then the verifier SHALL verify that the pre-registered telephone number being used is associated with a specific physical device. | 10/1/2024 | Agency | Both | Both |
| | | " | (20) If out-of-band verification is to be made using the PSTN, then changing the pre-registered telephone number is considered to be the binding of a new authenticator and SHALL only occur as described in IA-5 n (17) through (25). | 10/1/2024 | Agency | Both | Both |
| | | " | (21) If PSTN is used for out-of-band authentication, then the CSP SHALL offer subscribers at least one alternate authenticator that is not RESTRICTED and can be used to authenticate at the required AAL. | 10/1/2024 | Agency | Both | Both |
| | | " | (22) If PSTN is used for out-of-band authentication, then the CSP SHALL Provide meaningful notice to subscribers regarding the security risks of the RESTRICTED authenticator and availability of alternative(s) that are not RESTRICTED. | 10/1/2024 | Agency | Both | Both |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|----------------------------------------|----------------------------------------|------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|------|------|
| | | | | | IaaS | PaaS | SaaS |
| 5.6: IA-5 (1) | 5.6: IA-5 (1) | Authenticator Management Authenticator Types (continued) | (23) If PSTN is used for out-of-band authentication, then the CSP SHALL address any additional risk to subscribers in its risk assessment. | 10/1/2024 | Agency | Both | Both |
| | | " | (24) If PSTN is used for out-of-band authentication, then the CSP SHALL develop a migration plan for the possibility that the RESTRICTED authenticator is no longer acceptable at some point in the future and include this migration plan in its digital identity acceptance statement. | 10/1/2024 | Agency | Both | Both |
| | | " | (d) OTP Authenticators and Verifiers | | | | |
| | | " | (1) The secret key and its algorithm SHALL provide at least the minimum security strength of 112 bits as of the date of this publication. | 10/1/2024 | Agency | Both | Both |
| | | " | (2) The nonce SHALL be of sufficient length to ensure that it is unique for each operation of the device over its lifetime. | 10/1/2024 | Agency | Both | Both |
| | | " | (3) OTP authenticators — particularly software-based OTP generators — SHALL NOT facilitate the cloning of the secret key onto multiple devices. | 10/1/2024 | Agency | Both | Both |
| | | " | (4) The authenticator output SHALL have at least 6 decimal digits (approximately 20 bits) of entropy. | Current | Agency | Both | Both |
| | | " | (5) If the nonce used to generate the authenticator output is based on a real-time clock, then the nonce SHALL be changed at least once every 2 minutes. | 10/1/2024 | Agency | Both | Both |
| | | " | (6) The OTP value associated with a given nonce SHALL be accepted only once. | Current | Agency | Both | Both |
| | | " | (7) The symmetric keys used by authenticators are also present in the verifier and SHALL be strongly protected against compromise. | 10/1/2024 | Agency | Both | Both |
| | | " | (8) If a single-factor OTP authenticator is being associated with a subscriber account, then the verifier or associated CSP SHALL use approved cryptography to either generate and exchange or to obtain the secrets required to duplicate the authenticator output. | 10/1/2024 | Agency | Both | Both |
| | | " | (9) The verifier SHALL use approved encryption when collecting the OTP. | 10/1/2024 | Agency | Both | Both |
| | | " | (10) The verifier SHALL use an authenticated protected channel when collecting the OTP. | 10/1/2024 | Agency | Both | Both |
| | | " | (11) If a time-based OTP is used, it SHALL have a defined lifetime (recommended 30 seconds) that is determined by the expected clock drift — in either direction — of the authenticator over its lifetime, plus allowance for network delay and user entry of the OTP. | 10/1/2024 | Agency | Both | Both |
| | | " | (12) Verifiers SHALL accept a given time-based OTP only once during the validity period. | 10/1/2024 | Agency | Both | Both |
| | | " | (13) If the authenticator output has less than 64 bits of entropy, the verifier SHALL implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber's account as described in IA-5 I (3) through (4). | 10/1/2024 | Agency | Both | Both |
| | | " | (14) If the authenticator is multi-factor, then each use of the authenticator SHALL require the input of the additional factor. | 10/1/2024 | Agency | Both | Both |
| | | " | (15) If the authenticator is multi-factor and a memorized secret is used by the authenticator for activation, then that memorized secret SHALL be a randomly chosen numeric secret at least 6 decimal digits in length or other memorized secret meeting the requirements of IA-5 (1)(a). | 10/1/2024 | Agency | Both | Both |
| | | " | (16) If the authenticator is multi-factor, then use of a memorized secret for activation SHALL be rate limited as specified in IA-5 I (3) through (4). | 10/1/2024 | Agency | Both | Both |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|----------------------------------------|----------------------------------------|------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|------|------|
| | | | | | IaaS | PaaS | SaaS |
| 5.6: IA-5 (1) | 5.6: IA-5 (1) | Authenticator Management Authenticator Types (continued) | (17) If the authenticator is multi-factor and is activated by a biometric factor, then that factor SHALL meet the requirements of IA-5 m, including limits on the number of consecutive authentication failures. | 10/1/2024 | Agency | Both | Both |
| | | " | (18) If the authenticator is multi-factor, then the unencrypted key and activation secret or biometric sample — and any biometric data derived from the biometric sample such as a probe produced through signal processing — SHALL be zeroized immediately after an OTP has been generated. | 10/1/2024 | Agency | Both | Both |
| | | " | (19) If the authenticator is multi-factor, the verifier or CSP SHALL establish, via the authenticator source, that the authenticator is a multi-factor device. | 10/1/2024 | Agency | Both | Both |
| | | " | (20) In the absence of a trusted statement that it is a multi-factor device, the verifier SHALL treat the authenticator as single-factor, in accordance with IA-5 (1) (d) (1) through (13). | 10/1/2024 | Agency | Both | Both |
| | | " | (e) Cryptographic Authenticators and Verifiers (including single- and multi-factor cryptographic authenticators, both hardware- and software-based) | | | | |
| | | " | (1) If the cryptographic authenticator is software based, the key SHALL be stored in suitably secure storage available to the authenticator application. | 10/1/2024 | Agency | Both | Both |
| | | " | (2) If the cryptographic authenticator is software based, the key SHALL be strongly protected against unauthorized disclosure by the use of access controls that limit access to the key to only those software components on the device requiring access. | 10/1/2024 | Agency | Both | Both |
| | | " | (3) If the cryptographic authenticator is software based, it SHALL NOT facilitate the cloning of the secret key onto multiple devices. | 10/1/2024 | Agency | Both | Both |
| | | " | (4) If the authenticator is single-factor and hardware-based, secret keys unique to the device SHALL NOT be exportable (i.e., cannot be removed from the device). | 10/1/2024 | Agency | Both | Both |
| | | " | (5) If the authenticator is hardware-based, the secret key and its algorithm SHALL provide at least the minimum-security length of 112 bits as of the date of this publication. | 10/1/2024 | Agency | Both | Both |
| | | " | (6) If the authenticator is hardware-based, the challenge nonce SHALL be at least 64 bits in length. | 10/1/2024 | Agency | Both | Both |
| | | " | (7) If the authenticator is hardware-based, approved cryptography SHALL be used. | 10/1/2024 | Agency | Both | Both |
| | | " | (8) Cryptographic keys stored by the verifier SHALL be protected against modification. | 10/1/2024 | Agency | Both | Both |
| | | " | (9) If symmetric keys are used, cryptographic keys stored by the verifier SHALL be protected against disclosure. | 10/1/2024 | Agency | Both | Both |
| | | " | (10) The challenge nonce SHALL be at least 64 bits in length. | 10/1/2024 | Agency | Both | Both |
| | | " | (11) The challenge nonce SHALL either be unique over the authenticator's lifetime or statistically unique (i.e., generated using an approved random bit generator). | 10/1/2024 | Agency | Both | Both |
| | | " | (12) The verification operation SHALL use approved cryptography. | 10/1/2024 | Agency | Both | Both |
| | | " | (13) If a multi-factor cryptographic software authenticator is being used, then each authentication requires the presentation of the activation factor. | 10/1/2024 | Agency | Both | Both |
| | | " | (14) If the authenticator is multi-factor, then any memorized secret used by the authenticator for activation SHALL be a randomly chosen numeric secret at least 6 decimal digits in length or other memorized secret meeting the requirements of IA-5 (1) (a). | 10/1/2024 | Agency | Both | Both |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|----------------------------------------|----------------------------------------|------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|------|------|
| | | | | | IaaS | PaaS | SaaS |
| 5.6: IA-5 (1) | 5.6: IA-5 (1) | Authenticator Management Authenticator Types (continued) | (15) If the authenticator is multi-factor, then use of a memorized secret for activation SHALL be rate limited as specified in IA-5 I (3) through (4). | 10/1/2024 | Agency | Both | Both |
| | | " | (16) If the authenticator is multi-factor and is activated by a biometric factor, then that factor SHALL meet the requirements of IA-5 m, including limits on the number of consecutive authentication failures. | 10/1/2024 | Agency | Both | Both |
| | | " | (17) If the authenticator is multi-factor, then the unencrypted key and activation secret or biometric sample — and any biometric data derived from the biometric sample such as a probe produced through signal processing — SHALL be zeroized immediately after an authentication transaction has taken place. | 10/1/2024 | Agency | Both | Both |
| 5.6: IA-5 (2) | 5.6: IA-5 (2) | Authenticator Management Public Key Based Authentication | (a) For public key-based authentication: | | | | |
| | | " | (1) Enforce authorized access to the corresponding private key; and | Current | Agency | Both | Both |
| | | " | (2) Map the authenticated identity to the account of the individual or group; and | Current | Agency | Both | Both |
| | | " | (b) When public key infrastructure (PKI) is used: | Current | Agency | Both | Both |
| | | " | (1) Validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; and | Current | Agency | Both | Both |
| | | " | (2) Implement a local cache of revocation data to support path discovery and validation. | Current | Agency | Both | Both |
| 5.6: IA-5 (6) | 5.6: IA-5 (6) | Authenticator Management Protection of Authenticators | Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access. | Current | Agency | Both | Both |
| 5.6: IA-6 | 5.6: IA-6 | Authentication Feedback | Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals. | Current | Agency | Both | Both |
| 5.6: IA-7 | 5.6: IA-7 | Cryptographic Module Authentication | Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication. | 10/1/2024 | Agency | Both | Both |
| 5.6: IA-8 | 5.6: IA-8 | Identification and Authentication (Non-Organizational Users) | Control: Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users. | 10/1/2024 | Agency | Both | Both |
| 5.6: IA-8 (1) | 5.6: IA-8 (1) | Identification and Authentication (Non-Organizational Users) Acceptance of PIV Credentials From Other Agencies | Accept and electronically verify Personal Identity Verification-compliant credentials from other federal, state, local, tribal, or territorial (SLTT) agencies. | 10/1/2024 | Agency | Both | Both |
| 5.6: IA-8 (2) | 5.6: IA-8 (2) | Identification and Authentication (Non-Organizational Users) Acceptance of External Authenticators | (a) Accept only external authenticators that are NIST-compliant; and | 10/1/2024 | Agency | Both | Both |
| | | " | (b) Document and maintain a list of accepted external authenticators. | 10/1/2024 | Agency | Both | Both |
| 5.6: IA-8 (4) | 5.6: IA-8 (4) | Identification and Authentication (Non-Organizational Users) Use of Defined Profiles | Conform to the following profiles for identity management: Security Assertion Markup Language (SAML) or OpenID Connect. | 10/1/2024 | Agency | Both | Both |
| 5.6: IA-11 | 5.6: IA-11 | Re-Authentication | Require users to re-authenticate when: roles, authenticators, or credentials change, security categories of systems change, the execution of privileged functions occur, or every 12 hours. | 10/1/2024 | Agency | Both | Both |
| 5.6: IA-12 | 5.6: IA-12 | Identity Proofing | a. Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines; | 10/1/2024 | Agency | Both | Both |
| | | " | b. Resolve user identities to a unique individual; and | 10/1/2024 | Agency | Both | Both |
| | | " | c. Collect, validate, and verify identity evidence. | 10/1/2024 | Agency | Both | Both |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|----------------------------------------|----------------------------------------|-------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|------|------|
| | | | | | IaaS | PaaS | SaaS |
| 5.6: IA-12 (2) | 5.6: IA-12 (2) | Identity Proofing Identity Evidence | Require evidence of individual identification be presented to the registration authority. | 10/1/2024 | Agency | Both | Both |
| 5.6: IA-12 (3) | 5.6: IA-12 (3) | Identity Proofing Identity Evidence Validation and Verification | a. Require that the presented identity evidence be validated and verified through agency defined resolution, validation, and verification methods. | 10/1/2024 | Agency | Both | Both |
| | | " | b. Identity proofing SHALL NOT be performed to determine suitability or entitlement to gain access to services or benefits. | 10/1/2024 | Agency | Both | Both |
| | | " | c. 1. Collection of PII SHALL be limited to the minimum necessary to resolve to a unique identity in a given context. | 10/1/2024 | Agency | Both | Both |
| | | " | 2. Collection of PII SHALL be limited to the minimum necessary to validate the existence of the claimed identity and associate the claimed identity with the applicant providing identity evidence for appropriate identity resolution, validation, and verification. | 10/1/2024 | Agency | Both | Both |
| | | " | d. The CSP SHALL provide explicit notice to the applicant at the time of collection regarding the purpose for collecting and maintaining a record of the attributes necessary for identity proofing, including whether such attributes are voluntary or mandatory to complete the identity proofing process, and the consequences for not providing the attributes. | 10/1/2024 | Agency | Both | Both |
| | | " | e. If CSPs process attributes for purposes other than identity proofing, authentication, or attribute assertions (collectively "identity service"), related fraud mitigation, or to comply with law or legal process, then CSPs SHALL implement measures to maintain predictability and manageability commensurate with the privacy risk arising from the additional processing. | 10/1/2024 | Agency | Both | Both |
| | | " | f. If the CSP employs consent as part of its measures to maintain predictability and manageability, ...then it SHALL NOT make consent for the additional processing a condition of the identity service. | 10/1/2024 | Agency | Both | Both |
| | | " | g. The CSP SHALL provide mechanisms for redress of applicant complaints or problems arising from the identity proofing. | 10/1/2024 | Agency | Both | Both |
| | | " | These [redress] mechanisms SHALL be easy for applicants to find and use. | 10/1/2024 | Agency | Both | Both |
| | | " | h. The CSP SHALL assess the [redress] mechanisms for their efficacy in achieving resolution of complaints or problems. | 10/1/2024 | Agency | Both | Both |
| | | " | i. The identity proofing and enrollment processes SHALL be performed according to an applicable written policy or *practice statement* that specifies the particular steps taken to verify identities. | 10/1/2024 | Agency | Both | Both |
| | | " | j. The *practice statement* SHALL include control information detailing how the CSP handles proofing errors that result in an applicant not being successfully enrolled. | 10/1/2024 | Agency | Both | Both |
| | | " | k. The CSP SHALL maintain a record, including audit logs, of all steps taken to verify the identity of the applicant as long as the identity exists in the information system. | 10/1/2024 | Agency | Both | Both |
| | | " | l. The CSP SHALL record the types of identity evidence presented in the proofing process. | 10/1/2024 | Agency | Both | Both |
| | | " | m. The CSP SHALL conduct a risk management process, including assessments of privacy and security risks to determine: | 10/1/2024 | Agency | Both | Both |
| | | " | 1. Any steps that it will take to verify the identity of the applicant beyond any mandatory requirements specified herein; | 10/1/2024 | Agency | Both | Both |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|----------------------------------------|----------------------------------------|-------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|------|------|
| | | | | | IaaS | PaaS | SaaS |
| 5.6: IA-12 (3) | 5.6: IA-12 (3) | Identity Proofing Identity Evidence Validation and Verification (continued) | 2. The PII, including any biometrics, images, scans, or other copies of the identity evidence that the CSP will maintain as a record of identity proofing (Note: Specific federal requirements may apply); and | 10/1/2024 | Agency | Both | Both |
| | | " | 3. The schedule of retention for these records (Note: CSPs may be subject to specific retention policies in accordance with applicable laws, regulations, or policies, including any National Archives and Records Administration (NARA) records retention schedules that may apply). | 10/1/2024 | Agency | Both | Both |
| | | " | n. All PII collected as part of the enrollment process SHALL be protected to ensure confidentiality, integrity, and attribution of the information source. | 10/1/2024 | Agency | Both | Both |
| | | " | o. "The entire proofing transaction, including transactions that involve a third party, SHALL occur over authenticated protected channels. " | 10/1/2024 | Agency | Both | Both |
| | | " | p. "If the CSP uses fraud mitigation measures, then the CSP SHALL conduct a privacy risk assessment for these mitigation measures. " | 10/1/2024 | Agency | Both | Both |
| | | " | Such assessments SHALL include any privacy risk mitigations (e.g., risk acceptance or transfer, limited retention, use limitations, notice) or other technological mitigations (e.g., cryptography), and be documented per requirement IA-12(3) k – m above. | 10/1/2024 | Agency | Both | Both |
| | | " | q. In the event a CSP ceases to conduct identity proofing and enrollment processes, then the CSP SHALL be responsible for fully disposing of or destroying any sensitive data including PII, or its protection from unauthorized access for the duration of retention. | 10/1/2024 | Agency | Both | Both |
| | | " | r. Regardless of whether the CSP is a federal agency or non- federal entity, the following requirements apply to the federal agency offering or using the proofing service: | 10/1/2024 | Agency | Both | Both |
| | | " | 1. The agency SHALL consult with their Senior Agency Official for Privacy (SAOP) to conduct an analysis determining whether the collection of PII to conduct identity proofing triggers Privacy Act requirements. | 10/1/2024 | Agency | Both | Both |
| | | " | 2. The agency SHALL publish a System of Records Notice (SORN) to cover such collection, as applicable. | 10/1/2024 | Agency | Both | Both |
| | | " | 3. The agency SHALL consult with their SAOP to conduct an analysis determining whether the collection of PII to conduct identity proofing triggers E-Government Act of 2002 requirements. | 10/1/2024 | Agency | Both | Both |
| | | " | 4. The agency SHALL publish a Privacy Impact Assessment (PIA) to cover such collection, as applicable. | 10/1/2024 | Agency | Both | Both |
| | | " | s. An enrollment code SHALL be comprised of one of the following: | 10/1/2024 | Agency | Both | Both |
| | | " | 1. Minimally, a random six character alphanumeric or equivalent entropy. For example, a code generated using an approved random number generator or a serial number for a physical hardware authenticator; OR | 10/1/2024 | Agency | Both | Both |
| | | " | 2. A machine-readable optical label, such as a QR Code, that contains data of similar or higher entropy as a random six character alphanumeric. | 10/1/2024 | Agency | Both | Both |
| | | " | t. Training requirements for personnel validating evidence SHALL be based on the policies, guidelines, or requirements of the CSP or RP. | 10/1/2024 | Agency | Both | Both |
| | | " | u. This criterion applies to CSPs that provide identity proofing and enrollment services to minors (under the age of 18): | 10/1/2024 | Agency | Both | Both |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|----------------------------------------|----------------------------------------|-------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|------|------|
| | | | | | IaaS | PaaS | SaaS |
| 5.6: IA-12 (3) | 5.6: IA-12 (3) | Identity Proofing Identity Evidence Validation and Verification (continued) | If the CSP provides identity proofing and enrollment services to minors (under the age of 18), then...the CSP SHALL give special consideration to the legal restrictions of interacting with minors unable to meet the evidence requirements of identity proofing [to ensure compliance with the Children's Online Privacy Protection Act of 1998 (COPPA), and other laws, as applicable]. " | 10/1/2024 | Agency | Both | Both |
| | | " | Requirements v and w apply to the collection of biometric characteristics for in-person (physical or supervised remote) identity proofing and are mandatory at IAL3. These criteria also apply to CSPs that optionally choose to collect biometric characteristics through in-person identity-proofing identity proofing and enrollment at IAL2. | | | | |
| | | " | v. The CSP SHALL have the operator view the biometric source (e.g., fingers, face) for presence of non-natural materials and perform such inspections as part of the proofing process. | 10/1/2024 | Agency | Both | Both |
| | | " | w. The CSP SHALL collect biometrics in such a way that ensures that the biometric is collected from the applicant, and not another subject. All biometric performance requirements in IA-5 m (1) through (12) apply. | 10/1/2024 | Agency | Both | Both |
| | | " | x. The CSP SHALL support in-person or remote identity proofing, or both. | 10/1/2024 | Agency | Both | Both |
| | | " | y. The CSP SHALL collect the following from the applicant: | 10/1/2024 | Agency | Both | Both |
| | | " | 1. One piece of SUPERIOR or STRONG evidence if the evidence's issuing source, during its identity proofing event, confirmed the claimed identity by collecting two or more forms of SUPERIOR or STRONG evidence and the CSP validates the evidence directly with the issuing source; OR | 10/1/2024 | Agency | Both | Both |
| | | " | 2. Two pieces of STRONG evidence; OR | 10/1/2024 | Agency | Both | Both |
| | | " | 3. One piece of STRONG evidence plus two pieces of FAIR evidence | 10/1/2024 | Agency | Both | Both |
| | | " | z. The CSP SHALL validate each piece of evidence with a process that can achieve the same strength as the evidence presented (see 'z' above). For example, if two forms of STRONG identity evidence are presented, each piece of evidence will be validated at a strength of STRONG. | 10/1/2024 | Agency | Both | Both |
| | | " | aa. The CSP SHALL verify identity evidence as follows: | 10/1/2024 | Agency | Both | Both |
| | | " | At a minimum, the applicant's binding to identity evidence must be verified by a process that is able to achieve a strength of STRONG. | 10/1/2024 | Agency | Both | Both |
| | | " | bb. For IAL2 remote proofing: The collection of biometric characteristics for physical or biometric comparison of the applicant to the strongest piece of identity evidence provided to support the claimed identity performed remotely SHALL adhere to all requirements as specified in IA-5 m. | 10/1/2024 | Agency | Both | Both |
| | | " | cc. Knowledge-based verification (KBV) SHALL NOT be used for in-person (physical or supervised remote) identity verification. | 10/1/2024 | Agency | Both | Both |
| | | " | dd. The CSP SHALL employ appropriately tailored security controls, to include control enhancements, from the moderate or high baseline of security controls defined in the CJIS Security Policy. | 10/1/2024 | Agency | Both | Both |
| | | " | The CSP SHALL ensure that the minimum assurance-related controls for moderate-impact systems are satisfied. | 10/1/2024 | Agency | Both | Both |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|----------------------------------------|----------------------------------------|-------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|------|------|
| | | | | | IaaS | PaaS | SaaS |
| 5.6: IA-12 (3) | 5.6: IA-12 (3) | Identity Proofing Identity Evidence Validation and Verification (continued) | ee. Supervised Remote Identity Proofing: Supervised remote identity proofing is intended to provide controls for comparable levels of confidence and security to in-person IAL3 identity proofing for identity proofing processes that are performed remotely. Supervised remote identity proofing is optional for CSPs; that is, if a CSP chooses to use supervised remote identity proofing, then the following requirements, (1) through (8), would apply. It should be noted that the term “supervised remote identity proofing” has specialized meaning and is used only to refer to the specialized equipment and the following control requirements, (1) through (8). In addition to those requirements presented in this document, as well as the applicable identity validation and verification requirements, CSPs that provide supervised remote identity proofing services must demonstrate conformance with the requirements contained in this section. The following requirements for supervised remote proofing apply specifically to IAL3. If the equipment/facilities used for supervised remote proofing are used for IAL2 identity proofing, the following requirements, (1) through (8), for supervised remote proofing do not apply. In this case, the requirements for conventional remote identity proofing are applicable. | 10/1/2024 | Agency | Both | Both |
| | | " | (1) Supervised remote identity proofing and enrollment transactions SHALL meet the following requirements, in addition to the IAL3 validation and verification requirements specified in Section 4.6 . | 10/1/2024 | Agency | Both | Both |
| | | " | (2) The CSP SHALL monitor the entire identity proofing session, from which the applicant SHALL NOT depart — for example, by a continuous high-resolution video transmission of the applicant. | 10/1/2024 | Agency | Both | Both |
| | | " | (3) The CSP SHALL have a live operator participate remotely with the applicant for the entirety of the identity proofing session. | 10/1/2024 | Agency | Both | Both |
| | | " | (4) The CSP SHALL require all actions taken by the applicant during the identity proofing session to be clearly visible to the remote operator. | 10/1/2024 | Agency | Both | Both |
| | | " | (5) The CSP SHALL require that all digital validation of evidence (e.g., via chip or wireless technologies) be performed by integrated scanners and sensors. | 10/1/2024 | Agency | Both | Both |
| | | " | (6) The CSP SHALL require operators to have undergone a training program to detect potential fraud and to properly perform a supervised remote proofing session. | 10/1/2024 | Agency | Both | Both |
| | | " | (7) The CSP SHALL employ physical tamper detection and resistance features appropriate for the environment in which it is located. | 10/1/2024 | Agency | Both | Both |
| | | " | (8) The CSP SHALL ensure that all communications occur over a mutually authenticated protected channel. | 10/1/2024 | Agency | Both | Both |
| | | " | ff. Trusted Referee: The use of trusted referees is optional for CSPs; that is, if a CSP chooses to use trusted referees for identity proofing and enrollment, then the following requirements, (1) through (3) would apply. The use of trusted referees is intended to assist in the identity proofing and enrollment for populations that are unable to meet IAL2 identity proofing requirements, or otherwise would be challenged to perform identity proofing and enrollment process requirements. Such populations may include, but are not limited to: | 10/1/2024 | Agency | Both | Both |
| | | " | · disabled individuals; | 10/1/2024 | Agency | Both | Both |
| | | " | · elderly individuals; | 10/1/2024 | Agency | Both | Both |
| | | " | · homeless individuals, | 10/1/2024 | Agency | Both | Both |
| | | " | · individuals with little or no access to online services or computing devices; | 10/1/2024 | Agency | Both | Both |
| | | " | · unbanked and individuals with little or no credit history; | 10/1/2024 | Agency | Both | Both |
| | | " | · victims of identity theft; | 10/1/2024 | Agency | Both | Both |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|----------------------------------------|----------------------------------------|-------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|------|------|
| | | | | | IaaS | PaaS | SaaS |
| 5.6: IA-12 (3) | 5.6: IA-12 (3) | Identity Proofing Identity Evidence Validation and Verification (continued) | children under 18; and | 10/1/2024 | Agency | Both | Both |
| | | " | immigrants. | 10/1/2024 | Agency | Both | Both |
| | | " | In addition to those requirements presented in the General section of this document, as well as the applicable IAL requirements, CSPs that use trusted referees in their identity proofing services must demonstrate conformance with the requirements contained in this section. | | | | |
| | | " | (1) If the CSP uses trusted referees, then...The CSP SHALL establish written policy and procedures as to how a trusted referee is determined and the lifecycle by which the trusted referee retains their status as a valid referee, to include any restrictions, as well as any revocation and suspension requirements. | 10/1/2024 | Agency | Both | Both |
| | | " | (2) If the CSP uses trusted referees, then...The CSP SHALL proof the trusted referee at the same IAL as the applicant proofing. | 10/1/2024 | Agency | Both | Both |
| | | " | (3) If the CSP uses trusted referees, then...The CSP SHALL determine the minimum evidence required to bind the relationship between the trusted referee and the applicant. | 10/1/2024 | Agency | Both | Both |
| 5.6: IA-12 (5) | 5.6: IA-12 (5) | (5) Identity Proofing Address Confirmation | a. Require that a registration code <u>or</u> notice of proofing be delivered through an out-of-band channel to verify the users address (physical or digital) of record. | 10/1/2024 | Agency | Both | Both |
| | | " | b. The CSP SHALL confirm address of record. | 10/1/2024 | Agency | Both | Both |
| | | " | c. Valid records to confirm address SHALL be issuing source(s) or authoritative source(s). | 10/1/2024 | Agency | Both | Both |
| | | " | Self-asserted address data that has not been confirmed in records SHALL NOT be used for confirmation. | 10/1/2024 | Agency | Both | Both |
| | | " | d. Note that IAL2-7 applies only to in-person proofing at IAL2. | 10/1/2024 | Agency | Both | Both |
| | | " | If the CSP performs in-person proofing for IAL2 and provides an enrollment code directly to the subscriber for binding to an authenticator at a later time, then the enrollment code...SHALL be valid for a maximum of seven (7) days. | 10/1/2024 | Agency | Both | Both |
| | | " | e. For remote identity proofing at IAL2: | 10/1/2024 | Agency | Both | Both |
| | | " | The CSP SHALL send an enrollment code to a confirmed address of record for the applicant. | 10/1/2024 | Agency | Both | Both |
| | | " | f. For remote identity proofing at IAL2: | 10/1/2024 | Agency | Both | Both |
| | | " | The applicant SHALL present a valid enrollment code to complete the identity proofing process. | 10/1/2024 | Agency | Both | Both |
| | | " | g. Note that the following enrollment code validity periods apply to enrollment codes sent to confirmed addresses of record for IAL2 remote in-person proofing only. | 10/1/2024 | Agency | Both | Both |
| | | " | Enrollment codes shall have the following maximum validities: | 10/1/2024 | Agency | Both | Both |
| | | " | i. 10 days, when sent to a postal address of record within the contiguous United States; | 10/1/2024 | Agency | Both | Both |
| | | " | ii. 30 days, when sent to a postal address of record outside the contiguous United States; | 10/1/2024 | Agency | Both | Both |
| | | " | iii. 10 minutes, when sent to a telephone of record (SMS or voice); | 10/1/2024 | Agency | Both | Both |
| | | " | iv. 24 hours, when sent to an email address of record. | 10/1/2024 | Agency | Both | Both |
| | | " | h. If the enrollment code sent to the confirmed address of record as part of the remote identity proofing process at IAL2 is also intended to be an authentication factor, then...it SHALL be reset upon first use. | 10/1/2024 | Agency | Both | Both |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|----------------------------------------|----------------------------------------|----------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|------|------|
| | | | | | IaaS | PaaS | SaaS |
| 5.6: IA-12 (5) | 5.6: IA-12 (5) | (5) Identity Proofing Address Confirmation (continued) | i. If the CSP performs remote proofing at IAL2 and optionally sends notification of proofing in addition to sending the required enrollment code, then...The CSP SHALL ensure the enrollment code and notification of proofing are sent to different addresses of record. | 10/1/2024 | Agency | Both | Both |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|------------------------------------------------------------|----------------------------------------|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|------|------|
| | | | | | IaaS | PaaS | SaaS |
| CJIS Security Policy Section 5-7: Configuration Management | | | | | | | |
| 5.7.1.1 | 5.7.1.1 | Least Functionality | The agency shall configure the application, service, or information system to provide only essential capabilities and... | Current | Agency | Both | Both |
| | | " | ...and shall specifically prohibit and/or restrict the use of specified functions, ports, protocols, and/or services. | Current | Agency | Both | Both |
| 5.7.1.2 | 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. | Current | Agency | Both | Both |
| | | " | The network topological drawing shall include the following: | Current | | | |
| | | " | 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. | Current | Agency | Both | Both |
| | | " | 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. | Current | Agency | Both | Both |
| | | " | 3. "For Official Use Only" (FOUO) markings. | Current | Agency | Both | Both |
| | | " | 4. The agency name and date (day, month, and year) drawing was created or updated. | Current | Agency | Both | Both |
| 5.7.2 | 5.7.2 | Security of Configuration Documentation | Agencies shall protect the system documentation from unauthorized access consistent with the provisions described in section 5.5 Access Control. | Current | Agency | Both | Both |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|---------------------------------------------------------|----------------------------------------|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|--------|--------|
| | | | | | IaaS | PaaS | SaaS |
| CJIS Security Policy Section 5-8: Media Protection (MP) | | | | | | | |
| 5.8: MP-1 | 5.8: MP-1 | Policy and Procedures | a. Develop, document, and disseminate to authorized individuals: | Current | Agency | Agency | Agency |
| | | " | 1. Agency-level media protection policy that: | Current | Agency | Agency | Agency |
| | | " | (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance; and | Current | Agency | Agency | Agency |
| | | " | (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and | Current | Agency | Agency | Agency |
| | | " | 2. Procedures to facilitate the implementation of the media protection policy and the associated media protection controls; | Current | Agency | Agency | Agency |
| | | " | b. Designate an individual with security responsibilities to manage the development, documentation, and dissemination of the media protection policy and procedures; and | Current | Agency | Agency | Agency |
| | | " | c. Review and update the current media protection: | 10/1/2023 | Agency | Agency | Agency |
| | | " | 1. Policy at least annually and following any security incidents involving digital and/or non-digital media; and | 10/1/2023 | Agency | Agency | Agency |
| | | " | 2. Procedures at least annually and following any security incidents involving digital and/or non-digital media. | 10/1/2023 | Agency | Agency | Agency |
| 5.8: MP-2 | 5.8: MP-2 | Media Access | Restrict access to digital and non-digital media to authorized individuals. | Current | Both | Both | Both |
| 5.8: MP-3 | 5.8: MP-3 | Media Marking | a. Mark system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and | 10/1/2023 | Both | Both | Both |
| | | " | b. Exempt digital and non-digital media containing CJI from marking if the media remain within physically secure locations and controlled areas. | 10/1/2023 | Both | Both | Both |
| 5.8: MP-4 | 5.8: MP-4 | Media Storage | a. Physically control and securely store digital and non-digital media within physically secure locations or controlled areas and encrypt CJI on digital media when physical and personnel restrictions are not feasible; and | Current | Both | Both | Both |
| | | " | b. Protect system media types defined in MP-4a until the media are destroyed or sanitized using approved equipment, techniques, and procedures. | Current | Both | Both | Both |
| 5.8: MP-5 | 5.8: MP-5 | Media Transport | a. Protect and control digital and non-digital media to help prevent compromise of the data during transport outside of the physically secure locations or controlled areas using encryption, as defined in <u>Section 5.10.1.2 of this Policy</u> . Physical media will be protected at the same level as the information would be protected in electronic form. Restrict the activities associated with transport of electronic and physical media to authorized personnel; | Current | Agency | Both | Both |
| | | " | b. Maintain accountability for system media during transport outside of the physically secure location or controlled areas; | Current | Both | Both | Both |
| | | " | c. Document activities associated with the transport of system media; and | Current | Both | Both | Both |
| | | " | d. Restrict the activities associated with the transport of system media to authorized personnel. | Current | Both | Both | Both |
| 5.8: MP-6 | 5.8: MP-6 | Media Sanitization | a. Sanitize or destroy digital and non-digital media prior to disposal, release out of agency control, or release for reuse using overwrite technology at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media will be destroyed (cut up, shredded, etc.). Physical media will be securely disposed of when no longer needed for investigative or security purposes, whichever is later. Physical media will be destroyed by crosscut shredding or incineration; and | Current | Agency | Both | Both |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|----------------------------------------------|----------------------------------------------|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|-----------------------------------------|------|------|
| | | | | | IaaS | PaaS | SaaS |
| 5.8: MP-6 | 5.8: MP-6 | Media Sanitization (continued) | b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information. | Current | Agency | Both | Both |
| 5.8: MP-7 | 5.8: MP-7 | Media Use | a. Restrict the use of digital and non-digital media on agency-owned systems that have been approved for use in the storage, processing, or transmission of criminal justice information by using technical, physical, or administrative controls (examples below); and | 10/1/2023 | Agency | Both | Both |
| | | " | b. Prohibit the use of personally-owned digital media devices on all agency-owned or controlled systems that store, process, or transmit criminal justice information; and | 10/1/2023 | Agency | Both | Both |
| | | " | c. Prohibit the use of digital media devices on all agency-owned or controlled systems that store, process, or transmit criminal justice information when such devices have no identifiable owner. | 10/1/2023 | Agency | Both | Both |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|-------------------------------------------------------|----------------------------------------|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|------|------|
| | | | | | IaaS | PaaS | SaaS |
| CJIS Security Policy Section 5-9: Physical Protection | | | | | | | |
| 5.9 | 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. | Current | Both | Both | Both |
| 5.9.1.1 | 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. | Current | Both | Both | Both |
| | | " | Security perimeters shall be defined, controlled and secured in a manner acceptable to the CSA or SIB. | Current | Both | Both | Both |
| 5.9.1.2 | 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... | Current | Both | Both | Both |
| | | " | ...or shall issue credentials to authorized personnel. | Current | Both | Both | Both |
| 5.9.1.3 | 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... | Current | Both | Both | Both |
| | | " | ...and shall verify individual access authorizations before granting access. | Current | Both | Both | Both |
| 5.9.1.4 | 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. | Current | Both | Both | Both |
| 5.9.1.5 | 5.9.1.5 | Access Control for Display Medium | The agency shall control physical access to information system devices that display CJI and... | Current | Both | Both | Both |
| | | " | ...and shall position information system devices in such a way as to prevent unauthorized individuals from accessing and viewing CJI. | Current | Both | Both | Both |
| 5.9.1.6 | 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. | Current | Both | Both | Both |
| 5.9.1.7 | 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). | Current | Both | Both | Both |
| | | " | The agency shall escort visitors at all times and monitor visitor activity. | Current | Both | Both | Both |
| 5.9.1.8 | 5.9.1.8 | Delivery and Removal | The agency shall authorize and control information system-related items entering and exiting the physically secure location. | Current | Both | Both | Both |
| 5.9.2 | 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. | Current | Both | Both | Both |
| | | " | The agency shall , at a minimum: | Current | | | |
| | | " | 1. Limit access to the controlled area during CJI processing times to only those personnel authorized by the agency to access or view CJI. | Current | Both | Both | Both |
| | | " | 2. Lock the area, room, or storage container when unattended. | Current | Both | Both | Both |
| | | " | 3. Position information system devices and documents containing CJI in such a way as to prevent unauthorized individuals from access and view. | Current | Both | Both | Both |
| | | " | 4. Follow the encryption requirements found in section 5.10.1.1.2 for electronic storage (i.e. data “at rest”) of CJI. | Current | Both | Both | Both |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|--------------------------------------------------------------------------|----------------------------------------|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|------------------|------------------|
| | | | | | IaaS | PaaS | SaaS |
| CJIS Security Policy Section 5-10: Systems and Communications Protection | | | | | | | |
| 5.10.1 | 5.10.1 | Information Flow Enforcement | The network infrastructure shall control the flow of information between interconnected systems. | Current | Both | Service Provider | Service Provider |
| 5.10.1.1 | 5.10.1.1 | Boundary Protection | The agency shall : | Current | | | |
| | | " | 1. Control access to networks processing CJI. | Current | Both | Service Provider | Service Provider |
| | | " | 2. Monitor and control communications at the external boundary of the information system and at key internal boundaries within the system. | Current | Both | Service Provider | Service Provider |
| | | " | 3. 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. | Current | Both | Service Provider | Service Provider |
| | | " | 4. Employ tools and techniques to monitor network events, detect attacks, and provide identification of unauthorized use. | Current | Both | Service Provider | Service Provider |
| | | " | 5. 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 “fails closed” vs. “fails open”). | Current | Both | Service Provider | Service Provider |
| | | " | 6. 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. | Current | Both | Service Provider | Service Provider |
| 5.10.1.2.1 | 5.10.1.2.1 | Encryption for CJI in Transit | When CJI is transmitted outside the boundary of the physically secure location, the data shall be immediately protected via encryption. | Current | Both | Service Provider | Service Provider |
| | | " | When encryption is employed, the cryptographic module used shall be FIPS 140-2 certified and ... | Current | Both | Service Provider | Service Provider |
| | | " | ... and use a symmetric cipher key strength of at least 128 bit strength to protect CJI. | Current | Both | Service Provider | Service Provider |
| | | " | 2. Encryption shall not be required if the transmission medium meets all of the following requirements: | Current | | | |
| | | " | a. The agency owns, operates, manages, or protects the medium. | Current | Agency | Agency | Agency |
| | | " | b. Medium terminates within physically secure locations at both ends with no interconnections between. | Current | Agency | Agency | Agency |
| | | " | c. Physical access to the medium is controlled by the agency using the requirements in Section 5.9.1 and 5.12. | Current | Agency | Agency | Agency |
| | | " | d. Protection includes safeguards (e.g. acoustic, electric, electromagnetic, and physical) and if feasible countermeasures (e.g. alarms, notifications) to permit its use for the tranmission of unencrypted information through an area of lesser classification or control. | Current | Agency | Agency | Agency |
| | | " | e. With approval of the CSO. | Current | Agency | Agency | Agency |
| 5.10.1.2.2 | 5.10.1.2.2 | Encryption for CJI at Rest | When CJI is at rest (i.e. stored electronically) outside the boundary of the physically secure location, the data shall be protected via encryption. | Current | Both | Service Provider | Service Provider |
| | | " | When encryption is employed, agencies shall either encrypt CJI in accordance with the standard in Section 5.10.1.2.1 above, or ... | Current | Both | Service Provider | Service Provider |
| | | " | ... or use a symmetric cipher that is FIPS 197 certified (AES) and at least 256 bit strength. | Current | Both | Service Provider | Service Provider |
| | | " | 1. When agencies implement encryption on CJI at rest, the passphrase to unlock the cipher shall meet the following requirements: | Current | | | |
| | | " | a. Be at least 10 characters | Current | Both | Service Provider | Service Provider |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|----------------------------------------|----------------------------------------|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|------------------|------------------|
| | | | | | IaaS | PaaS | SaaS |
| 5.10.1.2.2 | 5.10.1.2.2 | Encryption for CJI at Rest (continued) | b. Not be a dictionary word | Current | Both | Service Provider | Service Provider |
| | | " | c. Include at least one (1) upper case letter, one (1) lower case letter, one (1) number, and one (1) special character | Current | Both | Service Provider | Service Provider |
| | | " | d. Be changed when previously authorized personnel no longer require access | Current | Both | Service Provider | Service Provider |
| | | " | 2. Multiple files maintained in the same unencrypted folder shall have separate and distinct passphrases. | Current | Both | Service Provider | Service Provider |
| | | " | 2. All audit requirements found in Section 5.4.1 Auditable Events and Content (Information Systems) shall be applied. | Current | Both | Service Provider | Service Provider |
| 5.10.1.2.3 | 5.10.1.2.3 | Public Key Infrastructure (PKI) Technology | For agencies using public key infrastructure (PKI) 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. | Current | Both | Service Provider | Service Provider |
| | | " | Registration to receive a public key certificate shall : | Current | | | |
| | | " | 1. Include authorization by a supervisor or a responsible official. | Current | Both | Service Provider | Service Provider |
| | | " | 2. Be accomplished by a secure process that verifies the identity of the certificate holder. | Current | Both | Service Provider | Service Provider |
| | | " | 3. Ensure the certificate is issued to the intended party. | Current | Both | Service Provider | Service Provider |
| 5.10.1.3 | 5.10.1.3 | Voice over Internet Protocol | 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: | Current | | | |
| | | " | 1. Establish usage restrictions and implementation guidance for VoIP technologies. | Current | Both | Service Provider | Service Provider |
| | | " | 2. Change the default administrative password on the IP phones and VoIP switches. | Current | Both | Service Provider | Service Provider |
| | | " | 3. Utilize Virtual Local Area Network (VLAN) technology to segment VoIP traffic from data traffic. | Current | Both | Service Provider | Service Provider |
| 5.10.1.4 | 5.10.1.4 | Cloud Computing | The storage of CJI, regardless of encryption status, shall only be permitted in cloud environments (e.g. government or third-party/commercial datacenters, etc.) which reside within the physical boundaries of APB-member country (i.e. U.S., U.S. territories, Indian Tribes, and Canada) and legal authority of an APB-member agency (i.e. U.S. – federal/state/territory, Indian Tribe, or the Royal Canadian Mounted Police (RCMP)). | Current | Service Provider | Service Provider | Service Provider |
| 5.10.1.4 | 5.10.1.4 | " | Metadata derived from unencrypted CJI shall be protected in the same manner as CJI and... | Current | Service Provider | Service Provider | Service Provider |
| | | " | ...and shall not be used for any advertising or other commercial purposes by any cloud service provider or other associated entity. | Current | Service Provider | Service Provider | Service Provider |
| 5.10.2 | 5.10.2 | Facsimile Transmission of CJI | 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. | Current | Both | Service Provider | Service Provider |
| 5.10.3.1 | 5.10.3.1 | Partitioning | The application, service, or information system shall separate user functionality (including user interface services) from information system management functionality. | Current | Both | Service Provider | Service Provider |
| | | " | 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). | Current | Both | Service Provider | Service Provider |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|----------------------------------------------|----------------------------------------------|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|-----------------------------------------|---------------------|---------------------|
| | | | | | IaaS | PaaS | SaaS |
| 5.10.3.2 | 5.10.3.2 | Virtualization | In addition to the security controls described in this policy, the following additional controls shall be implemented in a virtual environment: | Current | | | |
| | | " | 1. Isolate the host from the virtual machine. In other words, virtual machine users cannot access host files, firmware, etc. | Current | Both | Service Provider | Service Provider |
| | | " | 2. Maintain audit logs for all virtual machines and hosts and store the logs outside the hosts' virtual environment. | Current | Both | Service Provider | Service Provider |
| | | " | 3. Virtual Machines that are Internet facing (web servers, portal servers, etc.) shall be physically separate from Virtual Machines that process CJI internally or be separated by a virtual firewall. | Current | Both | Service Provider | Service Provider |
| | | " | 4. Drivers that serve critical functions shall be stored within the specific VM they service. In other words, do not store these drivers within the hypervisor, or host operating system, for sharing. Each VM is to be treated as an independent system - secured as independently as possible. | Current | Both | Service Provider | Service Provider |
| | | " | The following additional technical security controls shall be applied in virtual environments where CJI is comingled with non-CJI: | Current | | | |
| | | " | 1. Encrypt CJI when stored in a virtualized environment where CJI is comingled with non-CJI or segregate and store unencrypted CJI within its own secure VM. | Current | Both | Service Provider | Service Provider |
| | | " | 2. Encrypt network traffic within the virtual environment. | Current | Both | Service Provider | Service Provider |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|--------------------------------------------------|----------------------------------------|------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|----------|----------|
| | | | | | IaaS | PaaS | SaaS |
| CJIS Security Policy Section 5-11: Formal Audits | | | | | | | |
| 5.11.1.1 | 5.11.1.1 | Triennial Compliance Audits by the FBI CJIS Division | The CJIS Audit Unit (CAU) shall conduct a triennial audit of each CSA in order to verify compliance with applicable statutes, regulations and policies. | Current | CJIS/CSO | CJIS/CSO | CJIS/CSO |
| | | " | This audit shall include a sample of CJAs and, in coordination with the SIB, the NCJAs. | Current | CJIS/CSO | CJIS/CSO | CJIS/CSO |
| | | " | The FBI CJIS Division shall also have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities. | Current | CJIS/CSO | CJIS/CSO | CJIS/CSO |
| 5.11.1.2 | 5.11.1.2 | Triennial Security Audits by the FBI CJIS Division | This audit shall include a sample of CJAs and NCJAs. | Current | CJIS/CSO | CJIS/CSO | CJIS/CSO |
| 5.11.2 | 5.11.2 | Audits by the CSA | Each CSA shall : | Current | | | |
| | | " | 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. | Current | CJIS/CSO | CJIS/CSO | CJIS/CSO |
| | | " | 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. | Current | CJIS/CSO | CJIS/CSO | CJIS/CSO |
| | | " | 3. Have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities. | Current | CJIS/CSO | CJIS/CSO | CJIS/CSO |
| | | " | 4. Have the authority, on behalf of another CSA, to conduct a CSP compliance audit of contractor facilities and provide the results to the requesting CSA. If a subsequent CSA requests an audit of the same contractor facility, the CSA may provide the results of the previous audit unless otherwise notified by the requesting CSA that a new audit be performed. | Current | CJIS/CSO | CJIS/CSO | CJIS/CSO |
| 5.11.3 | 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. | Current | CJIS/CSO | CJIS/CSO | CJIS/CSO |
| | | " | The inspection team shall be appointed by the APB and... | Current | CJIS/CSO | CJIS/CSO | CJIS/CSO |
| | | " | ...and shall include at least one representative of the CJIS Division. | Current | CJIS/CSO | CJIS/CSO | CJIS/CSO |
| | | " | All results of the inquiry and audit shall be reported to the APB with appropriate recommendations. | Current | CJIS/CSO | CJIS/CSO | CJIS/CSO |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|-------------------------------------------------------|----------------------------------------|-------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|--------|--------|
| | | | | | IaaS | PaaS | SaaS |
| CJIS Security Policy Section 5-12: Personnel Security | | | | | | | |
| 5.12.1 | 5.12.1 | Personnel Screening Requirements for Individuals Requiring Unescorted Access to Unencrypted CJI | 1. To verify identification, state of residency and national fingerprint-based record checks shall be conducted prior to granting access to CJI for all personnel who have unescorted access to unencrypted CJI or unescorted access to physically secure locations or controlled areas (during times of CJI processing). | Current | Agency | Agency | Agency |
| | | " | 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. | Current | Agency | Agency | Agency |
| | | " | When appropriate, the screening shall be consistent with: | Current | Agency | Agency | Agency |
| | | " | a. 5 CFR 731.106; and/or | Current | Agency | Agency | Agency |
| | | " | b. Office of Personnel Management policy, regulations, and guidance; and/or | Current | Agency | Agency | Agency |
| | | " | c. agency policy, regulations, and guidance. | Current | Agency | Agency | Agency |
| | | " | 2. All requests for access shall be made as specified by the CSO. | Current | Agency | Agency | Agency |
| | | " | All CSO designees shall be from an authorized criminal justice agency. | Current | Agency | Agency | Agency |
| | | " | 3. If a record of any 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. | Current | Agency | Agency | Agency |
| | | " | a. If a felony conviction of any kind exists, the Interface Agency shall deny access to CJI. However, the Interface Agency 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. | Current | Agency | Agency | Agency |
| | | " | c. If a record of any kind is found on a contractor, the CGA shall be formally notified and system access shall be delayed pending review of the criminal history record information. | Current | Agency | Agency | Agency |
| | | " | c. (cont) The CGA shall in turn notify the contractor's security officer. | Current | Agency | Agency | Agency |
| | | " | 4. 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. | Current | Agency | Agency | Agency |
| | | " | 5. If the person already has access to CJI and is subsequently arrested and or convicted, continued access to CJI shall be determined by the CSO. | Current | Agency | Agency | Agency |
| | | " | 6. 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... | Current | Agency | Agency | Agency |
| | | " | ...and the person's appointing authority shall be notified in writing of the access denial. | Current | Agency | Agency | Agency |
| | | " | 7. The granting agency shall maintain a list of personnel who have been authorized unescorted access to unencrypted CJI and... | Current | Agency | Agency | Agency |
| | | " | ...and shall , upon request, provide a current copy of the access list to the CSO. | Current | Agency | Agency | Agency |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|----------------------------------------------|----------------------------------------------|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|-----------------------------------------|------|------|
| | | | | | IaaS | PaaS | SaaS |
| 5.12.2 | 5.12.2 | Personnel Termination | Upon termination of personnel by an interface agency, the agency shall immediately terminate access to local agency systems with access to CJI. | Current | Both | Both | Both |
| 5.12.2 | 5.12.2 | " | Furthermore, the interface agency shall provide notification or other action to ensure access to state and other agency systems is terminated. | Current | Both | Both | Both |
| 5.12.2 | 5.12.2 | " | If the employee is an employee of a NCJA or a Contractor, the employer shall notify all Interface Agencies that may be affected by the personnel change. | Current | Both | Both | Both |
| 5.12.3 | 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. | Current | Both | Both | Both |
| 5.12.4 | 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. | Current | Both | Both | Both |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|---------------------------------------------------|----------------------------------------|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|--------|--------|
| | | | | | IaaS | PaaS | SaaS |
| CJIS Security Policy Section 5-13: Mobile Devices | | | | | | | |
| 5.13 | 5.13 | Mobile Devices | The agency shall : | Current | | | |
| | | " | (i) establish usage restrictions and implementation guidance for mobile devices; | Current | Agency | Agency | Agency |
| | | " | (ii) authorize, monitor, control wireless access to the information system. | Current | Agency | Agency | Agency |
| 5.13.1.1 | 5.13.1.1 | 802.11 Wireless Protocols | Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) cryptographic algorithms, used by all pre-80.11i protocols, do not meet the requirements for FIPS 140-2 and shall not be used. | Current | Agency | Agency | Agency |
| | | " | Agencies shall implement the following controls for all agency-managed wireless access points with access to an agency's network that processes unencrypted CJI: | Current | | | |
| | | " | 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. | Current | Agency | Agency | Agency |
| | | " | 2. Maintain a complete inventory of all Access Points (APs) and 802.11 wireless devices. | Current | Agency | Agency | Agency |
| | | " | 3. Place APs in secured areas to prevent unauthorized physical access and user manipulation. | Current | Agency | Agency | Agency |
| | | " | 4. Test AP range boundaries to determine the precise extent of the wireless coverage and design the AP wireless coverage to limit the coverage area to only what is needed for operational purposes. | Current | Agency | Agency | Agency |
| | | " | 5. Enable user authentication and encryption mechanisms for the management interface of the AP. | Current | Agency | Agency | Agency |
| | | " | 6. Ensure that all APs have strong administrative passwords and ensure that all passwords are changed in accordance with section 5.6.3.1. | Current | Agency | Agency | Agency |
| | | " | 7. Ensure the reset function on APs is used only when needed and is only invoked by authorized personnel. Restore the APs to the latest security settings, when the reset functions are used, to ensure the factory default settings are not utilized. | Current | Agency | Agency | Agency |
| | | " | 8. Change the default service set identifier (SSID) in the APs. | Current | Agency | Agency | Agency |
| | | " | Disable the broadcast SSID feature so that the client SSID must match that of the AP. | Current | Agency | Agency | Agency |
| | | " | Validate that the SSID character string does not contain any agency identifiable information (division, department, street, etc.) or services. | Current | Agency | Agency | Agency |
| | | " | 9. Enable all security features of the wireless product, including the cryptographic authentication, firewall, and other privacy features. | Current | Agency | Agency | Agency |
| | | " | 10. Ensure that encryption key sizes are at least 128-bits and... | Current | Agency | Agency | Agency |
| | | " | ...and the default shared keys are replaced by unique keys. | Current | Agency | Agency | Agency |
| | | " | 11. Ensure that the ad hoc mode has been disabled. | Current | Agency | Agency | Agency |
| | | " | 12. Disable all nonessential management protocols on the APs. Disable non-FIPS compliant secure access to the management interface. | Current | Agency | Agency | Agency |
| | | " | 13. Ensure all management access and authentication occurs via FIPS compliant secure protocols (e.g. SFTP, HTTPS, SNMP over TLS, etc.). Disable non-FIPS compliant secure access to the management interface. | Current | Agency | Agency | Agency |
| | | " | 14. Enable logging (if supported) and... | Current | Agency | Agency | Agency |
| | | " | ...and review the logs on a recurring basis per local policy. | Current | Agency | Agency | Agency |
| | | " | At a minimum logs shall be reviewed monthly. | Current | Agency | Agency | Agency |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|----------------------------------------|----------------------------------------|---------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|--------|--------|
| | | | | | IaaS | PaaS | SaaS |
| 5.13.1.1 | 5.13.1.1 | 802.11 Wireless Protocols (continued) | 15. Insulate, virtually (e.g. virtual local area network (VLAN) and ACLs) or physically (e.g. firewalls), the wireless network from the operational wired infrastructure. | Current | Agency | Agency | Agency |
| | | " | 16. When disposing of access points that will no longer be used by the agency, clear access point configuration to prevent disclosure of network configuration, keys, passwords, etc. | Current | Agency | Agency | Agency |
| 5.13.1.2.1 | 5.13.1.2.1 | Cellular Service Abroad | When devices are authorized to access CJI outside the U.S., agencies shall perform an inspection to ensure that all controls are in place and functioning properly in accordance with the agency's policies prior to and after deployment outside of the U.S. | Current | Agency | Agency | Agency |
| 5.13.1.3 | 5.13.1.3 | Bluetooth | Organizational security policy shall be used to dictate the use of Bluetooth and its associated devices based on the agency's operational and business processes. | Current | Agency | Agency | Agency |
| 5.13.1.4 | 5.13.1.4 | Mobile Hotspots | When an agency allows mobile devices that are approved to access or store CJI to function as a Wi-Fi hotspot connecting to the Internet, they shall be configured: | Current | | | |
| | | " | 1. Enable encryption on the hotspot | Current | Agency | Agency | Agency |
| | | " | 2. Change the hotspot's default SSID | Current | Agency | Agency | Agency |
| | | " | a. Ensure the hotspot SSID does not identify the device make/model or agency ownership | Current | Agency | Agency | Agency |
| | | " | 3. Create a wireless network password (Pre-shared key) | Current | Agency | Agency | Agency |
| | | " | 4. Enable the hotspot's port filtering/blocking features if present | Current | Agency | Agency | Agency |
| | | " | 5. Only allow connections from agency controlled devices | Current | Agency | Agency | Agency |
| | | " | OR 1. Have a MDM solution to provide the same security as identified in 1 - 5 above. | Current | Agency | Agency | Agency |
| 5.13.2 | 5.13.2 | Mobile Device Management (MDM) | Devices that have had any unauthorized changes made to them (including but not limited to being rooted or jailbroken) shall not be used to process, store, or transmit CJI at any time. | Current | Agency | Agency | Agency |
| | | " | User agencies shall implement the following controls when directly accessing CJI from devices running limited feature operating system: | Current | | | |
| | | " | 1. Ensure that CJI is only transferred between CJI authorized applications and storage areas of the device. | Current | Agency | Agency | Agency |
| | | " | 2. MDM with centralized administration configured and implemented to perform at least the following controls: | Current | Agency | Agency | Agency |
| | | " | a. Remote locking of the device | Current | Agency | Agency | Agency |
| | | " | b. Remote wiping of the device | Current | Agency | Agency | Agency |
| | | " | c. Setting and locking device configuration | Current | Agency | Agency | Agency |
| | | " | d. Detection of "rooted" and "jailbroken" devices | Current | Agency | Agency | Agency |
| | | " | e. Enforcement of folder or disk level encryption | Current | Agency | Agency | Agency |
| | | " | f. Application of mandatory policy settings on the device | Current | Agency | Agency | Agency |
| | | " | g. Detection of unauthorized configurations | Current | Agency | Agency | Agency |
| | | " | h. Detection of unauthorized software or applications | Current | Agency | Agency | Agency |
| | | " | i. Ability to determine location of agency controlled devices | Current | Agency | Agency | Agency |
| | | " | j. Prevention of unpatched devices from accessing CJI or CJI systems | Current | Agency | Agency | Agency |
| | | " | k. Automatic device wiping after a specified number of failed access attempts | Current | Agency | Agency | Agency |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|----------------------------------------|----------------------------------------|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|--------|--------|
| | | | | | IaaS | PaaS | SaaS |
| 5.13.3 | 5.13.3 | Wireless Device Risk Mitigations | Organizations shall , as a minimum, ensure that wireless devices: | Current | | | |
| | | " | 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. | Current | Agency | Agency | Agency |
| | | " | 2. Are configured for local device authentication (see Section 5.13.8.1). | Current | Agency | Agency | Agency |
| | | " | 3. Use advanced authentication or CSO approved compensating controls as per Section 5.13.7.2.1. | Current | Agency | Agency | Agency |
| | | " | 4. Encrypt all CJI resident on the device. | Current | Agency | Agency | Agency |
| | | " | 5. Erase cached information, to include authenticators (see Section 5.6.2.1) in applications, when session is terminated. | Current | Agency | Agency | Agency |
| | | " | 6. Employ personal firewalls on full-featured operating system devices or run a Mobile Device Management (MDM) system that facilitates the ability to provide firewall services from the agency level. | Current | Agency | Agency | Agency |
| | | " | 7. Employ malicious code protection on full-featured operating system devices or run a MDM system that facilitates the ability to provide anti-malware services from the agency level. | Current | Agency | Agency | Agency |
| 5.13.4.1 | 5.13.4.1 | Patching/Updates | Agencies shall monitor mobile devices to ensure their patch and update state is current. | Current | Agency | Agency | Agency |
| 5.13.4.2 | 5.13.4.2 | Malicious Code Protection | Agencies that allow smartphones and tablets to access CJI shall have a process to approve the use of specific software or applications on the devices. | Current | Agency | Agency | Agency |
| 5.13.4.3 | 5.13.4.3 | Personal Firewall | A personal firewall shall be employed on all devices that have a full-feature operating system (i.e. laptops or tablets with Windows or Linux/Unix operating systems). | Current | Agency | Agency | Agency |
| | | " | At a minimum, the personal firewall shall perform the following activities: | Current | | | |
| | | " | 1. Manage program access to the Internet. | Current | Agency | Agency | Agency |
| | | " | 2. Block unsolicited requests to connect to the PC. | Current | Agency | Agency | Agency |
| | | " | 3. Filter Incoming traffic by IP address or protocol. | Current | Agency | Agency | Agency |
| | | " | 4. Filter Incoming traffic by destination ports. | Current | Agency | Agency | Agency |
| | | " | 5. Maintain an IP traffic log. | Current | Agency | Agency | Agency |
| 5.13.5 | 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. | Current | Agency | Agency | Agency |
| | | " | Special reporting procedures for mobile devices shall apply in any of the following situations: | Current | | | |
| | | " | 1. Loss of device control. For example: | Current | Agency | Agency | Agency |
| | | " | a. Device known to be locked, minimal duration of loss | Current | | | |
| | | " | b. Device lock state unknown, minimal duration of loss | Current | | | |
| | | " | c. Device lock state unknown, extended duration of loss | Current | | | |
| | | " | d. Device known to be unlocked, more than momentary duration of loss | Current | | | |
| | | " | 2. Total loss of device | Current | Agency | Agency | Agency |
| | | " | 3. Device compromise | Current | Agency | Agency | Agency |
| 5.13.6 | 5.13.6 | Access Control | Access control (Section 5.5 Access Control) shall be accomplished by the application that accesses CJI. | Current | Agency | Agency | Agency |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|----------------------------------------|----------------------------------------|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|--------|--------|
| | | | | | IaaS | PaaS | SaaS |
| 5.13.7.1 | 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. | Current | Agency | Agency | Agency |
| | | " | The authenticator used shall meet the requirements in section 5.6.2.1 Standard Authenticators. | Current | Agency | Agency | Agency |
| 5.13.7.2 | 5.13.7.2 | Advanced Authentication | When accessing CJI from an authorized mobile device, advanced authentication shall be used by the authorized user unless the access to CJI is indirect as described in Section 5.6.2.2.1. If access is indirect, then AA is not required. | Current | Agency | Agency | Agency |
| 5.13.7.2.1 | 5.13.7.2.1 | Compensating Controls | Before CSOs consider approval of compensating controls, Mobile Device Management (MDM) shall be implemented per Section 5.13.2. | Current | Agency | Agency | Agency |
| | | " | The compensating controls shall : | Current | | | |
| | | " | 1. Meet the intent of the CJIS Security Policy AA requirement | Current | Agency | Agency | Agency |
| | | " | 2. Provide a similar level of protection or security as the original AA requirement | Current | Agency | Agency | Agency |
| | | " | 3. Not rely upon the existing requirements for AA as compensating controls | Current | Agency | Agency | Agency |
| | | " | 4. Expire upon the CSO approved date or when a compliant AA solution is implemented. | Current | Agency | Agency | Agency |
| | | " | The following minimum controls shall be implemented as a part of the CSO approved compensating controls: | Current | | | |
| | | " | Possession and registration of an agency-issued smartphone or tablet as an indication it is the authorized user | Current | Agency | Agency | Agency |
| | | " | Use of device certificates as per Section 5.13.7.3 Device Certificates | Current | Agency | Agency | Agency |
| | | " | Implemented CJIS Security Policy compliant standard authenticator protection on the secure location where CJI is stored | Current | Agency | Agency | Agency |
| 5.13.7.3 | 5.13.7.3 | Device Certificates | When certificates or cryptographic keys used to authenticate a mobile device are used in lieu of compensating controls for advanced authentication, they shall be: | Current | | | |
| | | " | 1. Protected against being extracted from the device | Current | Agency | Agency | Agency |
| | | " | 2. Configured for remote wipe on demand or self-deletion based on a number of unsuccessful login or access attempts | Current | Agency | Agency | Agency |
| | | " | 3. Configured to use a secure authenticator (i.e. password, PIN) to unlock the key for use | Current | Agency | Agency | Agency |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|-------------------------------------------------------------------------|----------------------------------------|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|------|------|
| | | | | | IaaS | PaaS | SaaS |
| CJIS Security Policy Section 5-14: System and Services Acquisition (SA) | | | | | | | |
| 5.14: SA-22 | 5.14: SA-22 | UNSUPPORTED SYSTEM COMPONENTS | a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or | 10/1/2023 | Both | Both | Both |
| | | " | b. Provide the following option for alternative sources for continued support for unsupported components: original manufacturer support, or original contracted vendor support. | 10/1/2023 | Both | Both | Both |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|--------------------------------------------------------------------------|----------------------------------------|----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|------------------|------------------|
| | | | | | IaaS | PaaS | SaaS |
| CJIS Security Policy Section 5-15: System and Information Integrity (SI) | | | | | | | |
| 5.15: SI-1 | 5.15: SI-1 | POLICY AND PROCEDURES | a. Develop, document, and disseminate to all organizational personnel with system and information integrity responsibilities and information system owners: | 10/1/2023 | Agency | Agency | Agency |
| | | " | 1. Agency-level system and information integrity policy that: | 10/1/2023 | Agency | Agency | Agency |
| | | " | (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and | 10/1/2023 | Agency | Agency | Agency |
| | | " | (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and | 10/1/2023 | Agency | Agency | Agency |
| | | " | 2. Procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls; | 10/1/2023 | Agency | Agency | Agency |
| | | " | b. Designate organizational personnel with system and information integrity responsibilities to manage the development, documentation, and dissemination of the system and information integrity policy and procedures; and | 10/1/2023 | Agency | Agency | Agency |
| | | " | c. Review and update the current system and information integrity: | 10/1/2023 | Agency | Agency | Agency |
| | | " | 1. Policy annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI; and | 10/1/2023 | Agency | Agency | Agency |
| | | " | 2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI. | 10/1/2023 | Agency | Agency | Agency |
| 5.15: SI-2 | 5.15: SI-2 | FLAW REMEDIATION | a. Identify, report, and correct system flaws; | Current | Both | Service Provider | Service Provider |
| | | " | b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; | 10/1/2023 | Both | Service Provider | Service Provider |
| | | " | c. Install security-relevant software and firmware updates within the number of days listed after the release of the updates; | Current | Both | Service Provider | Service Provider |
| | | " | • Critical – 15 days | 10/1/2023 | Both | Service Provider | Service Provider |
| | | " | • High – 30 days | 10/1/2023 | Both | Service Provider | Service Provider |
| | | " | • Medium – 60 days | 10/1/2023 | Both | Service Provider | Service Provider |
| | | " | • Low – 90 days; and | 10/1/2023 | Both | Service Provider | Service Provider |
| | | " | d. Incorporate flaw remediation into the organizational configuration management process. | 10/1/2023 | Both | Service Provider | Service Provider |
| 5.15: SI-2 (2) | 5.15: SI-2 (2) | (2) FLAW REMEDIATION AUTOMATED FLAW REMEDIATION STATUS | Determine if system components have applicable security-relevant software and firmware updates installed using vulnerability scanning tools as least quarterly or following any security incidents involving CJI or systems used to process, store, or transmit CJI. | 10/1/2023 | Both | Service Provider | Service Provider |
| 5.15: SI-3 | 5.15: SI-3 | MALICIOUS CODE PROTECTION | a. Implement signature-based malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code; | 10/1/2023 | Both | Service Provider | Service Provider |
| | | " | b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures; | Current | Both | Service Provider | Service Provider |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|----------------------------------------|----------------------------------------|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|------------------|------------------|
| | | | | | IaaS | PaaS | SaaS |
| 5.15: SI-3 | 5.15: SI-3 | MALICIOUS CODE PROTECTION (continued) | c. Configure malicious code protection mechanisms to: | | | | |
| | | " | 1. Perform periodic scans of the system at least daily and real-time scans of files from external sources at network entry and exit points and on all servers and endpoint devices as the files are downloaded, opened, or executed in accordance with organizational policy; and | Current | Both | Service Provider | Service Provider |
| 5.15: SI-3 | 5.15: SI-3 | " | 2. Block or quarantine malicious code, take mitigating action(s), and when necessary, implement incident response procedures; and send alert to system/network administrators and/or organizational personnel with information security responsibilities in response to malicious code detection; and | 10/1/2023 | Both | Service Provider | Service Provider |
| | | " | d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system. | 10/1/2023 | Both | Service Provider | Service Provider |
| 5.15: SI-4 | 5.15: SI-4 | SYSTEM MONITORING | a. Monitor the system to detect: | 10/1/2023 | Both | Service Provider | Service Provider |
| | | " | 1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: | 10/1/2023 | Both | Service Provider | Service Provider |
| | | " | a. Intrusion detection and prevention | 10/1/2023 | Both | Service Provider | Service Provider |
| | | " | b. Malicious code protection | 10/1/2023 | Both | Service Provider | Service Provider |
| | | " | c. Vulnerability scanning | 10/1/2023 | Both | Service Provider | Service Provider |
| | | " | d. Audit record monitoring | 10/1/2023 | Both | Service Provider | Service Provider |
| | | " | e. Network monitoring | 10/1/2023 | Both | Service Provider | Service Provider |
| | | " | f. Firewall monitoring; | 10/1/2023 | Both | Service Provider | Service Provider |
| | | " | 2. Unauthorized local, network, and remote connections; | 10/1/2023 | Both | Service Provider | Service Provider |
| | | " | b. Identify unauthorized use of the system through the following techniques and methods: event logging (ref. 5.4 Audit and Accountability); | 10/1/2023 | Both | Service Provider | Service Provider |
| | | " | c. Invoke internal monitoring capabilities or deploy monitoring devices: | 10/1/2023 | Both | Service Provider | Service Provider |
| | | " | 1. Strategically within the system to collect organization-determined essential information; and | 10/1/2023 | Both | Service Provider | Service Provider |
| | | " | 2. At ad hoc locations within the system to track specific types of transactions of interest to the organization; | 10/1/2023 | Both | Service Provider | Service Provider |
| | | " | d. Analyze detected events and anomalies; | 10/1/2023 | Both | Service Provider | Service Provider |
| | | " | e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation; | 10/1/2023 | Both | Service Provider | Service Provider |
| | | " | f. Obtain legal opinion regarding system monitoring activities; and | 10/1/2023 | Both | Service Provider | Service Provider |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|----------------------------------------|----------------------------------------|-------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|------------------|------------------|
| | | | | | IaaS | PaaS | SaaS |
| 5.15: SI-4 | 5.15: SI-4 | SYSTEM MONITORING (continued) | g. Provide intrusion detection and prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring, and firewall monitoring software logs to organizational personnel with information security responsibilities weekly. | 10/1/2023 | Both | Service Provider | Service Provider |
| 5.15: SI-4 (2) | 5.15: SI-4 (2) | (2) SYSTEM MONITORING AUTOMATED TOOLS AND MECHANISMS FOR REAL-TIME ANALYSIS | Employ automated tools and mechanisms to support near-real-time analysis of events. | Current | Both | Service Provider | Service Provider |
| 5.15: SI-4 (4) | 5.15: SI-4 (4) | (4) SYSTEM MONITORING INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC | a. Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic; | Current | Both | Service Provider | Service Provider |
| | | " | b. Monitor inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions such as: the presence of malicious code or unauthorized use of legitimate code or credentials within organizational systems or propagating among system components, signaling to external systems, and the unauthorized exporting of information. | Current | Both | Service Provider | Service Provider |
| 5.15: SI-4 (5) | 5.15: SI-4 (5) | (5) SYSTEM MONITORING SYSTEM-GENERATED ALERTS | Alert organizational personnel with system monitoring responsibilities when the following system-generated indications of compromise or potential compromise occur: inappropriate or unusual activities with security or privacy implications. | Current | Both | Service Provider | Service Provider |
| 5.12: SI-5 | 5.12: SI-5 | SECURITY ALERTS, ADVISORIES, AND DIRECTIVES | a. Receive system security alerts, advisories, and directives from external source(s) (e.g., CISA, Multi-State Information Sharing & Analysis Center [MS-ISAC], U.S. Computer Emergency Readiness Team [USCERT], hardware/software providers, federal/state advisories, etc.) on an ongoing basis; | Current | Both | Service Provider | Service Provider |
| | | " | b. Generate internal security alerts, advisories, and directives as deemed necessary; | Current | Both | Service Provider | Service Provider |
| | | " | c. Issue security alerts, advisories, and directives to: organizational personnel implementing, operating, maintaining, and using the system; and | Current | Both | Service Provider | Service Provider |
| | | " | d. Implement security directives in accordance with established time frames, or notify the issuing organization of the degree of noncompliance. | 10/1/2023 | Both | Service Provider | Service Provider |
| 5.15: SI-7 | 5.15: SI-7 | SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | a. Employ integrity verification tools to detect unauthorized changes to software, firmware, and information systems that contain or process CJI; and | 10/1/2023 | Both | Service Provider | Service Provider |
| | | " | b. Take the following actions when unauthorized changes to the software, firmware, and information are detected: notify organizational personnel responsible for software, firmware, and/or information integrity and implement incident response procedures as appropriate. | 10/1/2023 | Both | Service Provider | Service Provider |
| | | (1) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY INTEGRITY CHECKS | Perform an integrity check of software, firmware, and information systems that contain or process CJI at agency-defined transitional states or security relevant events at least weekly or in an automated fashion. | 10/1/2023 | Both | Service Provider | Service Provider |
| | | (7) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY INTEGRATION OF DETECTION AND RESPONSE | Incorporate the detection of the following unauthorized changes into the organizational incident response capability: unauthorized changes to established configuration setting or the unauthorized elevation of system privileges. | 10/1/2023 | Both | Service Provider | Service Provider |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|----------------------------------------|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|------------------|------------------|
| | | | | | IaaS | PaaS | SaaS |
| 5.15: SI-8 | 5.15: SI-8 | SPAM PROTECTION | a. Employ spam protection mechanisms at system entry points to detect and act on unsolicited messages; and | Current | Both | Service Provider | Service Provider |
| | | " | b. Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures. | Current | Both | Service Provider | Service Provider |
| 5.15: SI-8 (2) | 5.15: SI-8 (2) | (2) SPAM PROTECTION AUTOMATIC UPDATES | Automatically update spam protection mechanisms at least daily. | 10/1/2023 | Both | Service Provider | Service Provider |
| 5.15: SI-10 | 5.15: SI-10 | INFORMATION INPUT VALIDATION | Check the validity of the following information inputs: all inputs to web/application servers, database servers, and any system or application input that might receive or process CJI. | 10/1/2023 | Both | Service Provider | Service Provider |
| 5.15: SI-11 | 5.15: SI-11 | ERROR HANDLING | a. Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited; and | 10/1/2023 | Both | Service Provider | Service Provider |
| | | " | b. Reveal error messages only to organizational personnel with information security responsibilities. | 10/1/2023 | Both | Service Provider | Service Provider |
| 5.15: SI-12 | 5.15: SI-12 | INFORMATION MANAGEMENT AND RETENTION | Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines and operational requirements. | Current | Both | Service Provider | Service Provider |
| 5.15: SI-16 | 5.15: SI-16 | (1) INFORMATION MANAGEMENT AND RETENTION LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS | Limit personally identifiable information being processed in the information life cycle to the minimum PII necessary to achieve the purpose for which it is collected (see Section 4.3). | Current | Both | Service Provider | Service Provider |
| | | (2) INFORMATION MANAGEMENT AND RETENTION MINIMIZE PERSONALLY IDENTIFIABLE INFORMATION IN TESTING, TRAINING, AND RESEARCH | Use the following techniques to minimize the use of personally identifiable information for research, testing, or training: data obfuscation, randomization, anonymization, or use of synthetic data. | 10/1/2023 | Both | Service Provider | Service Provider |
| | | (3) INFORMATION MANAGEMENT AND RETENTION INFORMATION DISPOSAL | Use the following techniques to dispose of, destroy, or erase information following the retention period: as defined in MP-6. | Current | Both | Service Provider | Service Provider |
| | | MEMORY PROTECTION | Implement the following controls to protect the system memory from unauthorized code execution: data execution prevention and address space layout randomization. | 10/1/2023 | Both | Service Provider | Service Provider |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | | | | |
|-----------------------------------------------------|----------------------------------------|---------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|--------------------------------------|------|------|-----------|--|--|
| | | | | | IaaS | PaaS | SaaS | | | |
| CJIS Security Policy Section 5-16: Maintenance (MA) | | | | | | | | | | |
| | MA-1 | POLICY AND PROCEDURES | a. Develop, document, and disseminate to organizational personnel with system maintenance responsibilities: | 10/1/2024 | | | | | | |
| | | " | 1. Agency-level maintenance policy that: | 10/1/2024 | | | | | | |
| | | " | (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and | 10/1/2024 | | | | | | |
| | | " | (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and | 10/1/2024 | | | | | | |
| | | " | 2. Procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls; | 10/1/2024 | | | | | | |
| | | " | b. Designate organizational personnel with information security and privacy responsibilities to manage the development, documentation, and dissemination of the maintenance policy and procedures; and | 10/1/2024 | | | | | | |
| | | " | c. Review and update the current maintenance: | 10/1/2024 | | | | | | |
| | | " | 1. Policy annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI; and | 10/1/2024 | | | | | | |
| | | " | 2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI. | 10/1/2024 | | | | | | |
| | MA-2 | CONTROLLED MAINTENANCE | a. Schedule, document, and review records of maintenance, repair, and replacement on system components in accordance with manufacturer or vendor specifications and/or organizational requirements; | 10/1/2024 | | | | | | |
| | | " | b. Approve and monitor all maintenance activities, whether performed on site or remotely and whether the system or system components are serviced on site or removed to another location; | 10/1/2024 | | | | | | |
| | | " | c. Require that organizational personnel with information security and privacy responsibilities explicitly approve the removal of the system or system components from organizational facilities for off-site maintenance, repair, or replacement; | 10/1/2024 | | | | | | |
| | | " | d. Sanitize equipment to remove information from associated media prior to removal from organizational facilities for off-site maintenance, repair, - replacement, or destruction; | 10/1/2024 | | | | | | |
| | | " | e. Check all potentially impacted controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions; and | 10/1/2024 | | | | | | |
| | | " | f. Include the following information in organizational maintenance records: | 10/1/2024 | | | | | | |
| | | " | 1. Component name | 10/1/2024 | | | | | | |
| | | " | 2. Component serial number | 10/1/2024 | | | | | | |
| | | " | 3. Date/time of maintenance | 10/1/2024 | | | | | | |
| | | " | 4. Maintenance performed | 10/1/2024 | | | | | | |
| | | " | 5. Name(s) of entity performing maintenance including escort if required. | 10/1/2024 | | | | | | |
| | | MA-3 | MAINTENANCE TOOLS | a. Approve, control, and monitor the use of system maintenance tools; and | | | | 10/1/2024 | | |
| | | | " | b. Review previously approved system maintenance tools prior to each use. | | | | 10/1/2024 | | |
| | MA-3(1) | (1) MAINTENANCE TOOLS / INSPECT TOOLS | Inspect the maintenance tools used by maintenance personnel for improper or unauthorized modifications. | 10/1/2024 | | | | | | |
| | MA-3(2) | (2) MAINTENANCE TOOLS / INSPECT MEDIA | Check media containing diagnostic and test programs for malicious code before the media are used in the system. | 10/1/2024 | | | | | | |

| Ver 5.9.2 Location and New Requirement | Ver 5.9.3 Location and New Requirement | Title | Shall Statement / Requirement | Audit / Sanction Date | Agency Responsibility by Cloud Model | | |
|----------------------------------------|----------------------------------------|-------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------|------|------|
| | | | | | IaaS | PaaS | SaaS |
| | MA-3(3) | (3) MAINTENANCE TOOLS / PREVENT UNAUTHORIZED REMOVAL | <i>Prevent the removal of maintenance equipment containing organizational information by:</i> | 10/1/2024 | | | |
| | | " | <i>(a) Verifying that there is no organizational information contained on the equipment;</i> | 10/1/2024 | | | |
| | | " | <i>(b) Sanitizing or destroying the equipment;</i> | 10/1/2024 | | | |
| | | " | <i>(c) Retaining the equipment within the facility; or</i> | 10/1/2024 | | | |
| | | " | <i>(d) Obtaining an exemption from organizational personnel with system maintenance responsibilities explicitly authorizing removal of the equipment from the facility.</i> | 10/1/2024 | | | |
| | MA-4 | NONLOCAL MAINTENANCE | <i>a. Approve and monitor nonlocal maintenance and diagnostic activities;</i> | 10/1/2024 | | | |
| | | " | <i>b. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system;</i> | 10/1/2024 | | | |
| | | " | <i>c. Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions;</i> | 10/1/2024 | | | |
| | | " | <i>d. Maintain records for nonlocal maintenance and diagnostic activities; and</i> | 10/1/2024 | | | |
| | | " | <i>e. Terminate session and network connections when nonlocal maintenance is completed.</i> | 10/1/2024 | | | |
| | MA-5 | MAINTENANCE PERSONNEL | <i>a. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel;</i> | 10/1/2024 | | | |
| | | " | <i>b. Verify that non-escorted personnel performing maintenance on the system possess the required access authorizations; and</i> | 10/1/2024 | | | |
| | | " | <i>c. Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.</i> | 10/1/2024 | | | |
| | MA-6 | TIMELY MAINTENANCE | <i>Obtain maintenance support and/or spare parts for critical system components that process, store, and transmit CJI within agency-defined recovery time and recovery point objectives of failure.</i> | 10/1/2024 | | | |