U. S. Department of Justice
Federal Bureau of Investigation
Criminal Justice Information Services Division

Requirements Companion Document to the FBI CJIS Security Policy Version 5.9.5

07/09/2024

Prepared by:
CJIS Information Security Officer

Recommended changes to version 5.9.4 of the *CJIS Security Policy (CSJISECPOL)* were approved by the Advisory Policy Board (APB) in November 2023 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 ***red bold italics*** and deleted language is indicated in ~~strikethrough~~.

The "Summary of Changes" page lists the sections with changes. Within the document and modifications are highlighted in yellow for ease of location.

Based on the "*CJISSECPOL* Security Control Priority and Implementation Deadlines" topic paper endorsed by the Fall 2023 APB and approved by the FBI Director, changes have been made to the "Audit / Sanction Date" column and a new "Priority" column has been added. The "Audit / Sanction Date" column indicates the date when modernized security controls will become sanctionable for audit. Requirements and modernized controls existing in *CJISSECPOL* version 5.9 are indicated in **GREEN** and state 'Existing'. New requirements modernized after that version are not yet sanctionable, indicated in **YELLOW**, and state "Zero-cycle". **The "Zero-cycle" begins for all agencies on October 1, 2024.** The "Priority" column indicates the approved assigned priority for each control. Priority 1 [P1] controls are immediately sanctionable upon publication of *CJISSECPOL* version 5.9.5 and marked as "Upon Pub" which means the date on the cover of the *CJISSECPOL* and this document.

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

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

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

Dark Gray	CJIS*/CSO
Dark Green	Agency
Dark Blue	Service Provider
Orange	Both
Aqua	TBD

Some modernized controls have not been assigned cloud matrix values and those corresponding cells are colored in Aqua and contain TBD.

* - CJIS means the FBI CJIS Division.

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

SUMMARY OF CHANGES

Version 5.9.5

1. **Section 5.7 Configuration Management, Fall 2023, APB#15, SA#3, Modernizing Configuration Management (CM) in the *CJISSECPOL***: modernize the CJIS Security Policy requirements for

   Configuration Management Policy and Procedures
   Baseline Configuration
   Configuration Change Control
   Impact Analyses
   Access Restrictions for Change
   Configuration Settings
   Least Functionality
   System Component Inventory
   Configuration Management Plan
   Software Usage Restrictions
   User-Installed Software
   Information Location

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy Sections 1 - 4 (Introduction, Approach, Roles & Responsibilities, and CJI/PII)								
1.3	1.3	Relationship to Local Security Policy and Other Policies	The local agency may complement the CJIS Security Policy with a local policy, or the agency may develop their own stand-alone security policy; however, the CJIS Security Policy **shall** always be the minimum standard and local policy may augment, or increase the standards,…	Existing	Existing	Agency	Agency	Agency
		"	...and local policy may augment, or increase the standards, but **shall not** detract from the CJIS Security Policy standards.	Existing	Existing	Agency	Agency	Agency
		"	The agency **shall** develop, disseminate, and maintain formal, documented procedures to facilitate the implementation of the CJIS Security Policy and, where applicable, the local security policy.	Existing	Existing	Agency	Agency	Agency
		"	The policies and procedures **shall** be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.	Existing	Existing	Agency	Agency	Agency
3.2.1	3.2.1	CJIS Systems Agencies (CSA)	The head of each CSA **shall** appoint a CJIS Systems Officer (CSO).	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
		"	Such decisions **shall** be documented and kept current.	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
3.2.1	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.	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
		"	The CSO **shall** set, maintain, and enforce the following:	Existing	Existing			
3.2.2(1)	3.2.2(1)	"	1. Standards for the selection, supervision, and separation of personnel who have access to CJI.	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
3.2.2(2)	3.2.2(2)	"	2. Policy governing the operation of computers, access devices, circuits, hubs, routers, firewalls, and other components that comprise and support a telecommunications network and related CJIS systems used to process, store, or transmit CJI, guaranteeing the priority, confidentiality, integrity, and availability of service needed by the criminal justice community.	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
		"	a. Ensure appropriate use, enforce system discipline, and ensure CJIS Division operating procedures are followed by all users of the respective services and information.	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
		"	b. Ensure state/federal agency compliance with policies approved by the APB and adopted by the FBI.	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
		"	c. Ensure the appointment of the CSA ISO and determine the extent of authority to the CSA ISO.	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
		"	d. Ensure the designation of a Terminal Agency Coordinator (TAC) within each agency with device access to CJIS systems.	Existing	Existing	Agency	Agency	Agency
		"	e. Ensure each agency having access to CJI has someone designated as the Local Agency Security Officer (LASO).	Existing	Existing	Agency	Agency	Agency
		"	f. Ensure the LASO receives enhanced security awareness training (ref. Section 5.2).	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
		"	g. Approve access to FBI CJIS systems.	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
		"	h. Assume ultimate responsibility for managing the security of CJIS systems within their state and/or agency.	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
		"	i. Perform other related duties outlined by the user agreements with the FBI CJIS Division.	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
3.2.3(3)	3.2.3(3)	"	3. Outsourcing of Criminal Justice Functions	Existing	Existing			
		"	a. Responsibility for the management of the approved security requirements **shall** remain with the CJA.	Existing	Existing	Agency	Agency	Agency
		"	b. Responsibility for the management control of network security **shall** remain with the CJA.	Existing	Existing	Agency	Agency	Agency
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.	Existing	Existing	Agency	Agency	Agency

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
3.2.7	3.2.7	Agency Coordinator (AC)	The AC **shall** be responsible for the supervision and integrity of the system, training and continuing education of employees and operators, scheduling of initial training and testing, and certification testing and all required reports by NCIC.	Existing	Existing	Agency	Agency	Agency
		"	The AC **shall**:	Existing	Existing			
		"	1. Understand the communications, records capabilities, and needs of the Contractor which is accessing federal and state records through or because of its relationship with the CGA.	Existing	Existing	Agency	Agency	Agency
		"	2. Participate in related meetings and provide input and comments for system improvement.	Existing	Existing	Agency	Agency	Agency
		"	3. Receive information from the CGA (e.g., system updates) and disseminate it to appropriate Contractor employees.	Existing	Existing	Agency	Agency	Agency
		"	4. Maintain and update manuals applicable to the effectuation of the agreement, and provide them to the Contractor.	Existing	Existing	Agency	Agency	Agency
		"	5. Maintain up-to-date records of Contractor's employees who access the system, including name, date of birth, social security number, date fingerprint card(s) submitted, date security clearance issued, and date initially trained, tested, certified or recertified (if applicable).	Existing	Existing	Agency	Agency	Agency
		"	6. Train or ensure the training of Contractor personnel. If Contractor personnel access NCIC, schedule the operators for testing or a certification exam with the CSA staff, or AC staff with permission from the CSA staff. Schedule new operators for the certification exam within six (6) months of assignment. Schedule certified operators for biennial re-certification testing within thirty (30) days prior to the expiration of certification. Schedule operators for other mandated class.	Existing	Existing	Agency	Agency	Agency
		"	7. The AC will not permit an untrained/untested or non-certified Contractor employee to access CJI or systems supporting CJI where access to CJI can be gained.	Existing	Existing	Agency	Agency	Agency
		"	8. Where appropriate, ensure compliance by the Contractor with NCIC validation requirements.	Existing	Existing	Agency	Agency	Agency
		"	9. Provide completed applicant fingerprint cards on each Contractor employee who accesses the system to the CJA (or, where appropriate, CSA) for criminal background investigation prior to such employee accessing the system.	Existing	Existing	Agency	Agency	Agency
		"	10. Any other responsibility for the AC promulgated by the FBI.	Existing	Existing	Agency	Agency	Agency
3.2.8	3.2.8	CJIS System Agency Information Secrurity Officer (CSA ISO)	The CSA ISO **shall**:	Existing	Existing			
		"	1. Serve as the security point of contact (POC) to the FBI CJIS Division ISO.	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
		"	2. Document technical compliance with the CJIS Security Policy with the goal to assure the confidentiality, integrity, and availability of criminal justice information to the user community throughout the CSA's user community, to include the local level.	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
		"	3. Document and provide assistance for implementing the security-related controls for the Interface Agency and its users.	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
		"	4. Establish a security incident response and reporting procedure to discover, investigate, document, and report to the CSA, the affected criminal justice agency, and the FBI CJIS Division ISO major incidents that significantly endanger the security or integrity of CJI.	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
3.2.9	3.2.9	Local Agency Security Officer (LASO)	Each LASO **shall**:	Existing	Existing			
		"	1. Identify who is using the CSA approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.	Existing	Existing	Agency	Agency	Agency
		"	2. Identify and document how the equipment is connected to the state system.	Existing	Existing	Agency	Agency	Agency
		"	3. Ensure that personnel security screening procedures are being followed as stated in this policy.	Existing	Existing	Agency	Agency	Agency
		"	4. Ensure the approved and appropriate security measures are in place and working as expected.	Existing	Existing	Agency	Agency	Agency
		"	5. Support policy compliance and ensure CSA ISO is promptly informed of security incidents.	Existing	Existing	Agency	Agency	Agency
3.2.10	3.2.10	FBI CJIS Division Information Security Officer (FBI CJIS ISO)	The FBI CJIS ISO **shall**:	Existing	Existing			
		"	1. Maintain the CJIS Security Policy.	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
		"	2. Disseminate the FBI Director approved CJIS Security Policy.	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
		"	3. Serve as a liaison with the CSA's ISO and with other personnel across the CJIS community and in this regard provide technical guidance as to the intent and implementation of operational and technical policy issues.	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
		"	4. Serve as a point-of-contact (POC) for computer incident notification and distribution of security alerts to the CSOs and ISOs.	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
		"	5. Assist with developing audit compliance guidelines as well as identifying and reconciling security-related issues.	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
		"	6. Develop and participate in information security training programs for the CSOs and ISOs, and provide a means by which to acquire feedback to measure the effectiveness and success of such training.	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
		"	7. Maintain a security policy resource center (SPRC) on FBI.gov and keep the CSOs and ISOs updated on pertinent information.	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
3.2.12	3.2.12	Compact Officer	Pursuant to the National Crime Prevention and Privacy Compact, each party state **shall** appoint a Compact Officer…	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
			...Compact Officer who **shall** ensure that Compact provisions and rules, procedures, and standards established by the Compact Council are complied with in their respective state.	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
4.2.1	4.2.1	Proper Access, Use, and Dissemination of CHRI	The III **shall** be accessed only for an authorized purpose.	Existing	Existing	Agency	Agency	Agency
		"	Further, CHRI **shall** only be used for an authorized purpose consistent with the purpose for which III was accessed.	Existing	Existing	Agency	Agency	Agency
4.2.2	4.2.2	Proper Access, Use, and Dissemination of NCIC Restricted Files Information	Proper access to, use, and dissemination of data from restricted files **shall** be consistent with the access, use, and dissemination policies concerning the III described in Title 28, Part 20, CFR, and the NCIC Operating Manual.	Existing	Existing	Agency	Agency	Agency
		"	The restricted files, which **shall** be protected as CHRI, are as follows:	Existing	Existing			
		"	1. Gang File	Existing	Existing	Agency	Agency	Agency
		"	2. Threat Screening Center File	Existing	Existing	Agency	Agency	Agency
		"	3. Supervised Release File	Existing	Existing	Agency	Agency	Agency
		"	4. National Sex Offender Registry File	Existing	Existing	Agency	Agency	Agency

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
4.2.2	4.2.2	Proper Access, Use, and Dissemination of NCIC Restricted Files Information (continued)	5. Historical Protection Order File of the NCIC	Existing	Existing	Agency	Agency	Agency
		"	6. Identity Theft File	Existing	Existing	Agency	Agency	Agency
		"	7. Protective Interest File	Existing	Existing	Agency	Agency	Agency
		"	8. Person With Information [PWI] data in the Missing Person Files	Existing	Existing	Agency	Agency	Agency
		"	9. Violent Person File	Existing	Existing	Agency	Agency	Agency
		"	10. NICS Denied Transaction File	Existing	Existing	Agency	Agency	Agency
4.2.3.2	4.2.3.2	For Other Authorized Purposes	Non-restricted files information **shall** not be disseminated commercially.	Existing	Existing	Agency	Agency	Agency
		"	Agencies **shall not** disseminate restricted files information for purposes other than law enforcement.	Existing	Existing	Agency	Agency	Agency
4.2.4	4.2.4	Storage	When CHRI is stored, agencies **shall** establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of the information.	Existing	Existing	Agency	Agency	Agency
		"	These records **shall** be stored for extended periods only when they are key elements for the integrity and/or utility of case files and/or criminal record files.	Existing	Existing	Agency	Agency	Agency
4.2.5.1	4.2.5.1	Justification	In addition to the use of purpose codes and logging information, all users **shall** provide a reason for all III inquiries whenever requested by NCIC System Managers, CSAs, local agency administrators, or their representatives.	Existing	Existing	Agency	Agency	Agency
4.3	4.3	Personally Identifiable Information (PII)	PII **shall** be extracted from CJI for the purpose of official business only.	Existing	Existing	Agency	Agency	Agency
		"	Agencies **shall** develop policies, based on state and local privacy rules, to ensure appropriate controls are applied when handling PII extracted from CJI.	Existing	Existing	Agency	Agency	Agency

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy Section 5-1: Information Exchange Agreements								
5.1	5.1	Policy Area 1: Information Exchange Agreements	The information shared through communication mediums **shall** be protected with appropriate security safeguards.	Existing	Existing	Agency	Agency	Agency
5.1.1	5.1.1	Information Exchange	Before exchanging CJI, agencies **shall** put formal agreements in place that specify security controls.	Existing	Existing	Agency	Agency	Agency
		"	Information exchange agreements for agencies sharing CJI data that is sent to and/or received from the FBI CJIS **shall** specify the security controls and conditions described in this document.	Existing	Existing	Agency	Agency	Agency
		"	Information exchange agreements **shall** be supported by documentation committing both parties to the terms of information exchange.	Existing	Existing	Agency	Agency	Agency
		"	Law Enforcement and civil agencies **shall** have a local policy to validate a requestor of CJI as an authorized recipient before disseminating CJI.	Existing	Existing	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.	Existing	Existing	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.	Existing	Existing	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.	Existing	Existing	Agency	Agency	Agency
		"	This agreement **shall** include the standards and sanctions governing utilization of CJIS systems.	Existing	Existing	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.	Existing	Existing	Agency	Agency	Agency
		"	All user agreements with the FBI CJIS Division **shall** be coordinated with the CSA head.	Existing	Existing	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.	Existing	Existing	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.	Existing	Existing	Agency	Agency	Agency
		"	These agreements **shall** include:	Existing	Existing			
		"	1. Audit.	Existing	Existing	Agency	Agency	Agency
		"	2. Dissemination.	Existing	Existing	Agency	Agency	Agency
		"	3. Hit confirmation.	Existing	Existing	Agency	Agency	Agency
		"	4. Logging.	Existing	Existing	Agency	Agency	Agency
		"	5. Quality Assurance (QA).	Existing	Existing	Agency	Agency	Agency
		"	6. Screening (Pre-Employment).	Existing	Existing	Agency	Agency	Agency
		"	7. Security.	Existing	Existing	Agency	Agency	Agency
		"	8. Timeliness.	Existing	Existing	Agency	Agency	Agency
		"	9. Training.	Existing	Existing	Agency	Agency	Agency
		"	10. Use of the system.	Existing	Existing	Agency	Agency	Agency
		"	11. Validation.	Existing	Existing	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.	Existing	Existing	Agency	Agency	Agency

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	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.	Existing	Existing	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.	Existing	Existing	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…	Existing	Existing	Both	Both	Both
		"	...and **shall** be subject to the same extent of audit review as are local user agencies.	Existing	Existing	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.	Existing	Existing	Both	Both	Both
		"	Modifications to the CJIS Security Addendum **shall** be enacted only by the FBI.	Existing	Existing	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.	Existing	Existing	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.	Existing	Existing	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).	Existing	Existing	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.	Existing	Existing	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.	Existing	Existing	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).	Existing	Existing	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.	Existing	Existing	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.	Existing	Existing	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.	Existing	Existing	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.	Existing	Existing	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.	Existing	Existing	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.	Existing	Existing	Agency	Agency	Agency

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	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).	Existing	Existing	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.	Existing	Existing	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.	Existing	Existing	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.	Existing	Existing	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.	Existing	Existing	Agency	Agency	Agency
		"	Each Channeler that directly accesses CJI **shall** also allow the FBI to conduct periodic penetration testing.	Existing	Existing	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…	Existing	Existing	Agency	Agency	Agency
		"	...and **shall** be subject to the same extent of audit review as are local user agencies.	Existing	Existing	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.	Existing	Existing	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.	Existing	Existing	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.	Existing	Existing	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…	Existing	Existing	Agency	Agency	Agency
		"	...and **shall** be subject to the same extent of audit review as are local user agencies.	Existing	Existing	Agency	Agency	Agency
5.1.2	5.1.2	Monitoring, Review, and Delivery of Services	As specified in the inter-agency agreements, MCAs, and contractual agreements with private contractors, the services, reports and records provided by the service provider **shall** be regularly monitored and reviewed.	Existing	Existing	Agency	Agency	Agency
		"	The CJA, authorized agency, or FBI **shall** maintain sufficient overall control and visibility into all security aspects to include, but not limited to, identification of vulnerabilities and information security incident reporting/response.	Existing	Existing	Agency	Agency	Agency
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.	Existing	Existing	Agency	Agency	Agency
5.1.2.1	5.1.2.1	Managing Changes to Service Providers	Any changes to services provided by a service provider **shall** be managed by the CJA, authorized agency, or FBI.	Existing	Existing	Agency	Agency	Agency
		"	Evaluation of the risks to the agency **shall** be undertaken based on the criticality of the data, system, and the impact of the change.	Existing	Existing	Agency	Agency	Agency

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
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.	Existing	Existing	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.	Existing	Existing	Agency	Agency	Agency

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy Section 5-2: 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:	Zero-cycle	P2	Both	Both	Both
		"	1. Organization-level awareness and training policy that:	Zero-cycle	P2	Both	Both	Both
		"	(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Zero-cycle	P2	Both	Both	Both
		"	(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and	Zero-cycle	P2	Both	Both	Both
		"	2. Procedures to facilitate the implementation of the awareness and training policy and the associated awareness and training controls;	Zero-cycle	P2	Both	Both	Both
		"	b. Designate organizational personnel with information security awareness and training responsibilities to manage the development, documentation, and dissemination of the awareness and training policy nd procedures; and	Zero-cycle	P2	Both	Both	Both
		"	c. Review and update the current awareness and training:	Zero-cycle	P2	Both	Both	Both
		"	1. Policy annually and following changes in the information system operating environment, when security incidents occur, or when changes to the CJIS Security Policy are made; and	Zero-cycle	P2	Both	Both	Both
		"	2. Procedures annually and following changes in the information system operating environment, when security incidents occur, or when changes to the CJIS Security Policy are made.	Zero-cycle	P2	Both	Both	Both
5.2: AT-2	5.2: AT-2	Literacy Training and Awareness	a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors):	Existing	P2	Both	Both	Both
		"	1. As part of initial training for new users prior to accessing CJI and annually thereafter; and	Existing	P2	Both	Both	Both
		"	2. When required by system changes or within 30 days of any security event for individuals involved in the event;	Existing	P2	Both	Both	Both
		"	b. Employ one or more of the following techniques to increase the security and privacy awareness of system users:	Existing	P2	Both	Both	Both
		"	1. Displaying posters	Existing	P2	TBD	TBD	TBD
		"	2. Offering supplies inscribed with security and privacy reminders	Existing	P2	TBD	TBD	TBD
		"	3. Displaying logon screen messages	Existing	P2	TBD	TBD	TBD
		"	4. Generating email advisories or notices from organizational officials	Existing	P2	TBD	TBD	TBD
		"	5. Conducting awareness events	Existing	P2	TBD	TBD	TBD
		"	c. Update literacy training and awareness content annually and following changes in the information system operating environment, when security incidents occur, or when changes are made in the CJIS Security Policy; and	Existing	P2	Both	Both	Both
		"	d. Incorporate lessons learned from internal or external security incidents or breaches into literacy training and awareness techniques.	Existing	P2	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.	Existing	P2	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.	Existing	P2	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:	Existing	P2	Both	Both	Both
		"	· All individuals with unescorted access to a physically secure location;	Existing	P2	Both	Both	Both

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
		ROLE-BASED TRAINING (continued)	· General User: A user, but not a process, who is authorized to use an information system;	Existing	P2	Both	Both	Both
		"	· Privileged User: A user that is authorized (and, therefore, trusted) to perform security-relevant functions that general users are not authorized to perform:	Existing	P2	Both	Both	Both
		"	1. Before authorizing access to the system, information, or performing assigned duties, and annually thereafter; and	Existing	P2	Both	Both	Both
		"	2. When required by system changes;	Existing	P2	Both	Both	Both
		"	b. Update role-based training content annually and following audits of the CSA and local agencies ; changes in the information system operating environment; security incidents; or when changes are made to the CJIS Security Policy;	Existing	P2	Both	Both	Both
		"	c. Incorporate lessons learned from internal or external security incidents or breaches into role-based training;	Existing	P2	Both	Both	Both
		"	d. Incorporate the minimum following topics into the appropriate role-based training content:	Existing	P2	Both	Both	Both
		"	1. All individuals with unescorted access to a physically secure location:	Existing	P2			
		"	a. Access, Use and Dissemination of Criminal History Record Information (CHRI), NCIC Restricted Files Information, and NCIC Non-Restricted Files Information Penalties	Existing	P2	Both	Both	Both
		"	b. Reporting Security Events	Existing	P2	Both	Both	Both
		"	c. Training	Existing	P2	Both	Both	Both
		"	d. System Use Notification	Existing	P2	Both	Both	Both
		"	e. Physical Access Authorizations	Existing	P2	Both	Both	Both
		"	f. Physical Access Control	Existing	P2	Both	Both	Both
5.2: AT-3	5.2: AT-3	"	g. Monitoring Physical Access	Existing	P2	Both	Both	Both
		"	h. Visitor Control	Existing	P2	Both	Both	Both
		"	i. Personnel Sanctions	Existing	P2	Both	Both	Both
		"	2. General User: A user, but not a process, who is authorized to use an information system. In addition to AT-3 (d) (1) above, include the following topics:	Existing	P2			
		"	a. Criminal Justice Information	Existing	P2	Both	Both	Both
		"	b. Proper Access, Use, and Dissemination of NCIC Non-Restricted Files Information	Existing	P2	Both	Both	Both
		"	c. Personally Identifiable Information	Existing	P2	Both	Both	Both
		"	d. Information Handling	Existing	P2	Both	Both	Both
		"	e. Media Storage	Existing	P2	Both	Both	Both
		"	f. Media Access	Existing	P2	Both	Both	Both
		"	g. Audit Monitoring, Analysis, and Reporting	Existing	P2	Both	Both	Both
		"	h. Access Enforcement	Existing	P2	Both	Both	Both
		"	i. Least Privilege	Existing	P2	Both	Both	Both
		"	j. System Access Control	Existing	P2	Both	Both	Both
		"	k. Access Control Criteria	Existing	P2	Both	Both	Both
		"	l. System Use Notification	Existing	P2	Both	Both	Both
		"	m. Session Lock	Existing	P2	Both	Both	Both
		"	n. Personally Owned Information Systems	Existing	P2	Both	Both	Both
		"	o. Password	Existing	P2	Both	Both	Both
		"	p. Access Control for Display Medium	Existing	P2	Both	Both	Both
		"	q. Encryption	Existing	P2	Both	Both	Both

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
5.2: AT-3	5.2: AT-3	ROLE-BASED TRAINING (continued)	r. Malicious Code Protection	Existing	P2	Both	Both	Both
		"	s. Spam and Spyware Protection	Existing	P2	Both	Both	Both
		"	t. Cellular Devices	Existing	P2	Both	Both	Both
		"	u. Mobile Device Management	Existing	P2	Both	Both	Both
		"	v. Wireless Device Risk Mitigations	Existing	P2	Both	Both	Both
		"	w. Wireless Device Malicious Code Protection	Existing	P2	Both	Both	Both
		"	x. Literacy Training and Awareness/Social Engineering and Mining	Existing	P2	Both	Both	Both
		"	y. Identification and Authentication (Organizational Users)	Existing	P2	Both	Both	Both
		"	z. Media Protection	Existing	P2	Both	Both	Both
		"	3. Privileged User: A user that is authorized (and, therefore, trusted) to perform security-relevant functions that general users are not authorized to perform. In addition to AT-3 (d) (1) and (2) above, include the following topics:	Existing	P2			
		"	a. Access Control	Existing	P2	Both	Both	Both
		"	b. System and Communications Protection and Information Integrity	Existing	P2	Both	Both	Both
		"	c. Patch Management	Existing	P2	Both	Both	Both
		"	d. Data backup and storage—centralized or decentralized approach	Existing	P2	Both	Both	Both
		"	e. Most recent changes to the CJIS Security Policy	Existing	P2	Both	Both	Both
		"	4. Organizational Personnel with Security Responsibilities: Personnel with the responsibility to ensure the confidentiality, integrity, and availability of CJI and the implementation of technology in a manner compliant with the CJISSECPOL. In addition to AT-3 (d) (1), (2), and (3) above, include the following topics:	Existing	P2			
		"	a. Local Agency Security Officer Role	Existing	P2	Both	Both	Both
			b. Authorized Recipient Security Officer Role	Zero-cycle	P2	Both	Both	Both
		"	c. Additional state/local/tribal/federal agency LASO roles and responsibilities	Existing	P2	Both	Both	Both
		"	d. Summary of audit findings from previous state audits of local agencies	Existing	P2	Both	Both	Both
		"	e. Findings from the last FBI CJIS Division audit	Existing	P2	Both	Both	Both
5.2: AT-3 (5)	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.	Zero-cycle	P2	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	Existing	P4	Both	Both	Both
		"	b. Retain individual training records for a minimum of three years.	Existing	P4	Both	Both	Both

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy Section 5-3: Incident Response (IR)								
IR-1	IR-1	POLICY AND PROCEDURES	a. Develop, document, and disseminate to all personnel when their unescorted logical or physical access to any information system results in the ability, right, or privilege to view, modify, or make use of unencrypted CJI:	Existing	P2	Both	Both	Both
		"	1. Agency-level incident response policy that:	Existing	P2	Both	Both	Both
		"	(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Existing	P2	Both	Both	Both
		"	(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and	Existing	P2	Both	Both	Both
		"	2. Procedures to facilitate the implementation of the incident response policy and the associated incident response controls;	Existing	P2	Both	Both	Both
		"	b. Designate an individual with security responsibilities to manage the development, documentation, and dissemination of the incident response policy and procedures; and	Existing	P2	Both	Both	Both
		"	c. Review and update the current incident response:	Zero-cycle	P2	Both	Both	Both
		"	1. Policy annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI; and	Zero-cycle	P2	Both	Both	Both
		"	2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.	Zero-cycle	P2	Both	Both	Both
IR-2	IR-2	INCIDENT RESPONSE TRAINING	a. Provide incident response training to system users consistent with assigned roles and responsibilities:	Existing	P2	Both	Both	Both
		"	1. Prior to assuming an incident response role or responsibility or acquiring system access;	Existing	P2	Both	Both	Both
		"	2. When required by system changes; and	Existing	P2	Both	Both	Both
		"	3. Annually thereafter; and	Existing	P2	Both	Both	Both
		"	b. Review and update incident response training content annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.	Zero-cycle	P3	Both	Both	Both
IR-2 (3)	IR-2 (3)	(3) INCIDENT RESPONSE TRAINING | BREACH	Provide incident response training on how to identify and respond to a breach, including the organization's process for reporting a breach.	Zero-cycle	P3	Both	Both	Both
IR-3	IR-3	INCIDENT RESPONSE TESTING	Test the effectiveness of the incident response capability for the system annually using the following tests: tabletop or walk-through exercises; simulations; or other agency-appropriate tests.	Zero-cycle	P3	Both	Both	Both
IR-3 (2)	IR-3 (2)	(2) INCIDENT RESPONSE TESTING | COORDINATION WITH RELATED PLANS	Coordinate incident response testing with organizational elements responsible for related plans.	Zero-cycle	P3	Both	Both	Both
IR-4	IR-4	INCIDENT HANDLING	a. Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery;	Existing	P2	Both	Both	Both
		"	b. Coordinate incident handling activities with contingency planning activities;	Existing	P2	Both	Both	Both
		"	c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly; and	Existing	P2	Both	Both	Both
		"	d. Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.	Existing	P2	Both	Both	Both
IR-4 (1)	IR-4 (1)	(1) INCIDENT HANDLING | AUTOMATED INCIDENT HANDLING PROCESSES	Support the incident handling process using automated mechanisms (e.g., online incident management systems and tools that support the collection of live response data, full network packet capture, and forensic analysis.	Existing	P2	Both	Both	Both

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
IR-5	IR-5	INCIDENT MONITORING	Track and document incidents.	Existing	P2	Both	Both	Both
IR-6	IR-6	INCIDENT REPORTING	a. Require personnel to report suspected incidents to the organizational incident response capability immediately but not to exceed one (1) hour after discovery; and	Zero-cycle	P2	Both	Both	Both
		"	b. Report incident information to organizational personnel with incident handling responsibilities, and if confirmed, notify the CSO, SIB Chief, or Interface Agency Official.	Zero-cycle	P2	Both	Both	Both
IR-6 (1)	IR-6 (1)	(1) INCIDENT REPORTING | AUTOMATED REPORTING	Report incidents using automated mechanisms.	Existing	P2	Both	Both	Both
IR-6 (3)	IR-6 (3)	(3) INCIDENT REPORTING | SUPPLY CHAIN COORDINATION	Provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident.	Zero-cycle	P2	Both	Both	Both
IR-7	IR-7	INCIDENT RESPONSE ASSISTANCE	Provide an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the system for the handling and reporting of incidents.	Existing	P3	Both	Both	Both
IR-7 (1)	IR-7 (1)	(1) INCIDENT RESPONSE ASSISTANCE | AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION AND SUPPORT	Increase the availability of incident response information and support using automated mechanisms described in the discussion.	Zero-cycle	P3	Both	Both	Both
IR-8	IR-8	INCIDENT RESPONSE PLAN	a. Develop an incident response plan that:	Existing	P2	Both	Both	Both
		"	1. Provides the organization with a roadmap for implementing its incident response capability;	Existing	P2	Both	Both	Both
		"	2. Describes the structure and organization of the incident response capability;	Existing	P2	Both	Both	Both
		"	3. Provides a high-level approach for how the incident response capability fits into the overall organization;	Existing	P2	Both	Both	Both
		"	4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;	Existing	P2	Both	Both	Both
		"	5. Defines reportable incidents;	Existing	P2	Both	Both	Both
		"	6. Provides metrics for measuring the incident response capability within the organization;	Existing	P2	Both	Both	Both
		"	7. Defines the resources and management support needed to effectively maintain and mature an incident response capability;	Existing	P2	Both	Both	Both
		"	8. Addresses the sharing of incident information;	Existing	P2	Both	Both	Both
		"	9. Is reviewed and approved by the organization's/agency's executive leadership annually; and	Existing	P2	Both	Both	Both
		"	10. Explicitly designates responsibility for incident response to organizational personnel with incident reporting responsibilities and CSO or CJIS WAN Official.	Existing	P2	Both	Both	Both
		"	b. Distribute copies of the incident response plan to organizational personnel with incident handling responsibilities;	Existing	P2	Both	Both	Both
		"	c. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing;	Existing	P2	Both	Both	Both
		"	d. Communicate incident response plan changes to organizational personnel with incident handling responsibilities; and	Existing	P2	Both	Both	Both
		"	e. Protect the incident response plan from unauthorized disclosure and modification.	Existing	P2	Both	Both	Both

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
IR-8 (1)	IR-8 (1)	(1) INCIDENT RESPONSE PLAN | BREACHES	Include the following in the Incident Response Plan for breaches involving personally identifiable information:	Zero-cycle	P2	Both	Both	Both
		"	(a) A process to determine if notice to individuals or other organizations, including oversight organizations, is needed;	Zero-cycle	P2	Both	Both	Both
		"	(b) An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms; and	Zero-cycle	P2	Both	Both	Both
		"	(c) Identification of applicable privacy requirements.	Zero-cycle	P2	Both	Both	Both

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy Section 5-4: Audit and Accountability								
AU-1	AU-1	POLICY AND PROCEDURES	a. Develop, document, and disseminate to organizational personnel with audit and accountability responsibilities:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. Agency and system-level audit and accountability policy that:	Zero-cycle	P2	TBD	TBD	TBD
		"	(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Zero-cycle	P2	TBD	TBD	TBD
		"	(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and	Zero-cycle	P2	TBD	TBD	TBD
		"	2. Procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls;	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Designate organizational personnel with information security responsibilities to manage the development, documentation, and dissemination of the audit and accountability policy and procedures; and	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Review and update the current audit and accountability:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. Policy annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI; and	Zero-cycle	P2	TBD	TBD	TBD
		"	2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.	Zero-cycle	P2	TBD	TBD	TBD
AU-2	AU-2	EVENT LOGGING	a. Identify the types of events that the system is capable of logging in support of the audit function: authentication, file use, user/group management, events sufficient to establish what occurred, the sources of events, outcomes of events, and operational transactions (e.g., NCIC, III);	Existing	P2	Both	Both	Service Provider
		"	b. Coordinate the event logging function with other organizational entities requiring audit- related information to guide and inform the selection criteria for events to be logged;	Existing	P2	Both	Both	Service Provider
		"	c. Specify the following event types for logging within the system:	Existing	P2	Both	Both	Service Provider
		"	All successful and unsuccessful:	Existing	P2	Both	Both	Service Provider
		"	1. System log-on attempts	Existing	P2	Both	Both	Service Provider
		"	2. Attempts to use:	Existing	P2	Both	Both	Service Provider
		"	a. Access permission on a user account, file, directory, or other system resource;	Existing	P2	Both	Both	Service Provider
		"	b. Create permission on a user account, file, directory, or other system resource;	Existing	P2	Both	Both	Service Provider
		"	c. Write permission on a user account, file, directory, or other system resource;	Existing	P2	Both	Both	Service Provider
		"	d. Delete permission on a user account, file, directory, or other system resource;	Existing	P2	Both	Both	Service Provider
		"	e. Change permission on a user account, file, directory, or other system resource.	Existing	P2	Both	Both	Service Provider
		"	3. Attempts to change account passwords	Existing	P2	Both	Both	Service Provider
		"	4. Actions by privileged accounts (i.e., root, Oracle, DBA, admin, etc.)	Existing	P2	Both	Both	Service Provider

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
AU-2	AU-2	EVENT LOGGING (continued)	5. Attempts for users to:	Existing	P2	Both	Both	Service Provider
		"	a. Access the audit log file;	Existing	P2	Both	Both	Service Provider
		"	b. Modify the audit log file;	Existing	P2	Both	Both	Service Provider
		"	c. Destroy the audit log file;	Existing	P2	Both	Both	Service Provider
		"	d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and	Existing	P2	Both	Both	Service Provider
		"	e. Review and update the event types selected for logging annually.	Existing	P2	Both	Both	Service Provider
AU-3	AU-3	CONTENT OF AUDIT RECORDS	Ensure that audit records contain information that establishes the following:	Existing	P2	Both	Both	Service Provider
		"	a. What type of event occurred;	Existing	P2	Both	Both	Service Provider
		"	b. When the event occurred;	Existing	P2	Both	Both	Service Provider
		"	c. Where the event occurred;	Existing	P2	Both	Both	Service Provider
		"	d. Source of the event;	Existing	P2	Both	Both	Service Provider
		"	e. Outcome of the event; and	Existing	P2	Both	Both	Service Provider
		"	f. Identity of any individuals, subjects, or objects/entities associated with the event.	Existing	P2	Both	Both	Service Provider
AU-3 (1)	AU-3 (1)	(1) CONTENT OF AUDIT RECORDS | ADDITIONAL AUDIT INFORMATION	Generate audit records containing the following additional information:	Existing	P2	Both	Both	Service Provider
		"	a. Session, connection, transaction, and activity duration;	Existing	P2	Both	Both	Service Provider
		"	b. Source and destination addresses;	Existing	P2	Both	Both	Service Provider
		"	c. Object or filename involved; and	Existing	P2	Both	Both	Service Provider
		"	d. Number of bytes received and bytes sent (for client-server transactions) in the audit records for audit events identified by type, location, or subject.	Existing	P2	Both	Both	Service Provider
		"	e. The III portion of the log shall clearly identify:	Existing	P2	Both	Both	Service Provider
		"	1. The operator	Existing	P2	Agency	Agency	Agency
		"	2. The authorized receiving agency	Existing	P2	Agency	Agency	Agency
		"	3. The requestor	Existing	P2	Agency	Agency	Agency
		"	4. The secondary recipient	Existing	P2	Agency	Agency	Agency
AU-3 (3)	AU-3 (3)	(3) CONTENT OF AUDIT RECORDS | LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS	Limit personally identifiable information contained in audit records to the following elements identified in the privacy risk assessment: minimum PII necessary to achieve the purpose for which it is collected (see Section 4.3).	Zero-cycle	P2	TBD	TBD	TBD
AU-4	AU-4	AUDIT LOG STORAGE CAPACITY	Allocate audit log storage capacity to accommodate the collection of audit logs to meet retention requirements (AU-11).	Zero-cycle	P2	TBD	TBD	TBD

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
AU-5	AU-5	RESPONSE TO AUDIT LOGGING PROCESS FAILURES	a. Alert organizational personnel with audit and accountability responsibilities and system/network administrators within one (1) hour in the event of an audit logging process failure; and	Existing	P2	Both	Both	Both
		"	b. Take the following additional actions: restart all audit logging processes and verify system(s) are logging properly.	Existing	P2	Both	Both	Both
AU-6	AU-6	AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING	a. Review and analyze system audit records weekly for indications of inappropriate or unusual activity and the potential impact of the inappropriate or unusual activity;	Existing	P2	Both	Both	Both
		"	b. Report findings to organizational personnel with audit review, analysis, and reporting responsibilities and organizational personnel with information security and privacy responsibilities; and	Existing	P2	Both	Both	Both
		"	c. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.	Existing	P2	Both	Both	Both
AU-6 (1)	AU-6 (1)	(1) AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | AUTOMATED PROCESS INTEGRATION	Integrate audit record review, analysis, and reporting processes using automated mechanisms.	Zero-cycle	P2	TBD	TBD	TBD
AU-6 (3)	AU-6 (3)	(3) AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | CORRELATE AUDIT RECORD REPOSITORIES	Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.	Zero-cycle	P2	TBD	TBD	TBD
AU-7	AU-7	AUDIT RECORD REDUCTION AND REPORT GENERATION	a. Supports on-demand audit record review, analysis, and reporting requirements and after- the-fact investigations of incidents; and	Zero-cycle	P3	TBD	TBD	TBD
		"	b. Does not alter the original content or time ordering of audit records.	Zero-cycle	P3	TBD	TBD	TBD
AU-7 (1)	AU-7 (1)	(1) AUDIT RECORD REDUCTION AND REPORT GENERATION | AUTOMATIC PROCESSING	Provide and implement the capability to process, sort, and search audit records for events of interest based on the following content: information included in AU-3.	Zero-cycle	P3	TBD	TBD	TBD
AU-8	AU-8	TIME STAMPS	a. Use internal system clocks to generate time stamps for audit records;	Existing	P2	Both	Both	Service Provider
		"	b. Record time stamps for audit records that meet hundredths of a second (i.e., hh:mm:ss:00) interval and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.	Existing	P2	Both	Both	Service Provider
AU-9	AU-9	PROTECTION OF AUDIT INFORMATION	a. Protect audit information and audit logging tools from unauthorized access, modification, and deletion; and	Existing	P2	Both	Both	Service Provider
		"	b. Alert organizational personnel with audit and accountability responsibilities, organizational personnel with information security and privacy responsibilities, and system/network administrators upon detection of unauthorized access, modification, or deletion of audit information.	Existing	P2	Both	Both	Service Provider
AU-9 (4)	AU-9 (4)	(4) PROTECTION OF AUDIT INFORMATION | ACCESS BY SUBSET OF PRIVILEGED USERS	Authorize access to management of audit logging functionality to only organizational personnel with audit and accountability responsibilities, organizational personnel with information security and privacy responsibilities, and system/network administrators.	Zero-cycle	P2	TBD	TBD	TBD
AU-11	AU-11	AUDIT RECORD RETENTION	Retain audit records for a minimum of one (1) year or until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.	Existing	P4	Both	Both	Service Provider

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
AU-12	AU-12	AUDIT RECORD GENERATION	a. Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on all systems generating required audit logs;	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Allow organizational personnel with audit record generation responsibilities, organizational personnel with information security and privacy responsibilities, and system/network administrators to select the event types that are to be logged by specific components of the system; and	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Generate audit records for the event types defined in AU-2c that include the audit record content defined in AU-3.	Zero-cycle	P2	TBD	TBD	TBD

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy Section 5-5: Access Control (AC)								
AC-1	AC-1	POLICY AND PROCEDURES	a. Develop, document, and disseminate to: organizational personnel with access control responsibilities	Zero-cycle	P2	Agency	Both	Both
		"	1. Agency-level access control policy that:	Zero-cycle	P2	Agency	Both	Both
		"	(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Zero-cycle	P2	Agency	Both	Both
		"	(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and	Zero-cycle	P2	Agency	Both	Both
		"	2. Procedures to facilitate the implementation of the access control policy and the associated access controls;	Zero-cycle	P2	Agency	Both	Both
		"	b. Designate an individual with security responsibilities to manage the development, documentation, and dissemination of the access control policy and procedures; and	Zero-cycle	P2	Agency	Both	Both
		"	c. Review and update the current access control:	Zero-cycle	P2	Agency	Both	Both
		"	1. Policy annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI; and	Zero-cycle	P2	Agency	Both	Both
		"	2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.	Zero-cycle	P2	Agency	Both	Both
AC-2	AC-2	ACCOUNT MANAGEMENT	a. Define and document the types of accounts allowed and specifically prohibited for use within the system;	Existing	P1	Agency	Both	Both
		"	b. Assign account managers;	Existing	P1	Agency	Both	Both
		"	c. Require conditions for group and role membership;	Existing	P1	Agency	Both	Both
		"	d. Specify:	Existing	P1	Agency	Both	Both
		"	1. Authorized users of the system;	Existing	P1	Agency	Both	Both
		"	2. Group and role membership; and	Existing	P1	Agency	Both	Both
		"	3. Access authorizations (i.e., privileges) and attributes listed for each account;	10/1/2024	P1	Agency	Both	Both
		"	Attribute Name	10/1/2024	P1	Agency	Both	Both
		"	Email Address Text	10/1/2024	P1	Agency	Both	Both
		"	Employer Name	10/1/2024	P1	Agency	Both	Both
		"	Federation Id	10/1/2024	P1	Agency	Both	Both
		"	Given Name	10/1/2024	P1	Agency	Both	Both
		"	Identity Provider Id	10/1/2024	P1	Agency	Both	Both
		"	Sur Name	10/1/2024	P1	Agency	Both	Both
		"	Telephone Number	10/1/2024	P1	Agency	Both	Both
		"	Identity Provider Id	10/1/2024	P1	Agency	Both	Both
		"	Unique Subject Id	10/1/2024	P1	Agency	Both	Both
		"	Counter Terrorism Data Self Search Home Privilege Indicator	10/1/2024	P1	Agency	Both	Both
		"	Criminal History Data Self Search Home Privilege Indicator	10/1/2024	P1	Agency	Both	Both
		"	Criminal Intelligence Data Self Search Home Privilege Indicator	10/1/2024	P1	Agency	Both	Both
		"	Criminal Investigative Data Self Search Home Privilege Indicator	10/1/2024	P1	Agency	Both	Both
		"	Display Name	10/1/2024	P1	Agency	Both	Both
		"	Government Data Self Search Home Privilege Indicator	10/1/2024	P1	Agency	Both	Both
		"	Local Id	10/1/2024	P1	Agency	Both	Both
		"	NCIC Certification Indicator	10/1/2024	P1	Agency	Both	Both
		"	NDEx Privilege Indicator	10/1/2024	P1	Agency	Both	Both
		"	PCII Certification Indicator	10/1/2024	P1	Agency	Both	Both
		"	28 CFR Certification Indicator	10/1/2024	P1	Agency	Both	Both
		"	Employer ORI	10/1/2024	P1	Agency	Both	Both
		"	Employer Organization General Category Code	10/1/2024	P1	Agency	Both	Both

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
AC-2	AC-2	ACCOUNT MANAGEMENT (continued)	Employer State Code	10/1/2024	P1	Agency	Both	Both
		"	Public Safety Officer Indicator	10/1/2024	P1	Agency	Both	Both
		"	Sworn Law Enforcement Officer Indicator	10/1/2024	P1	Agency	Both	Both
		"	Authenticator Assurance Level	10/1/2024	P1	Agency	Both	Both
		"	Federation Assurance Level	10/1/2024	P1	Agency	Both	Both
		"	Identity Assurance Level	10/1/2024	P1	Agency	Both	Both
		"	Intelligence Analyst Indicator	10/1/2024	P1	Agency	Both	Both
		"	e. Require approvals by organizational personnel with account management responsibilities for requests to create accounts;	Existing	P1	Agency	Both	Both
		"	f. Create, enable, modify, disable, and remove accounts in accordance with agency policy;	Existing	P1	Agency	Both	Both
		"	g. Monitor the use of accounts;	Existing	P1	Agency	Both	Both
		"	h. Notify account managers and system/network administrators within:	10/1/2024	P1	Agency	Both	Both
		"	1. One day when accounts are no longer required;	10/1/2024	P1	Agency	Both	Both
		"	2. One day when users are terminated or transferred; and	10/1/2024	P1	Agency	Both	Both
		"	3. One day when system usage or need-to-know changes for an individual;	10/1/2024	P1	Agency	Both	Both
		"	i. Authorize access to the system based on:	Existing	P1	Agency	Both	Both
		"	1. A valid access authorization;	Existing	P1	Agency	Both	Both
		"	2. Intended system usage; and	Existing	P1	Agency	Both	Both
		"	3. Attributes as listed in AC-2(d)(3);	10/1/2024	P1	Agency	Both	Both
		"	j. Review accounts for compliance with account management requirements at least annually;	Existing	P1	Agency	Both	Both
		"	k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and	Existing	P1	Agency	Both	Both
		"	l. Align account management processes with personnel termination and transfer processes.	Existing	P1	Agency	Both	Both
AC-2(1)	AC-2(1)	(1) ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT	Support the management of system accounts using automated mechanisms including email, phone, and text notifications.	10/1/2024	P1	Agency	Both	Both
AC-2(2)	AC-2(2)	(2) ACCOUNT MANAGEMENT | AUTOMATED TEMPORARY AND EMERGENCY ACCOUNT MANAGEMENT	Automatically remove temporary and emergency accounts within 72 hours.	10/1/2024	P1	Agency	Both	Both
AC-2(3)	AC-2(3)	(3) ACCOUNT MANAGEMENT | DISABLE ACCOUNTS	Disable accounts within one (1) week when the accounts:	10/1/2024	P1	Agency	Both	Both
		"	(a) Have expired;	10/1/2024	P1	Agency	Both	Both
		"	(b) Are no longer associated with a user or individual;	10/1/2024	P1	Agency	Both	Both
		"	(c) Are in violation of organizational policy; or	10/1/2024	P1	Agency	Both	Both
		"	(d) Have been inactive for 90 calendar days.	10/1/2024	P1	Agency	Both	Both
AC-2(4)	AC-2(4)	(4) ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS	Automatically audit account creation, modification, enabling, disabling, and removal actions.	Existing	P1	Agency	Both	Both
AC-2(5)	AC-2(5)	(5) ACCOUNT MANAGEMENT | INACTIVITY LOGOUT	Require that users log out when a work period has been completed.	10/1/2024	P1	Agency	Both	Both
AC-2(13)	AC-2(13)	(13) ACCOUNT MANAGEMENT | DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS	Disable accounts of individuals within 30 minutes of discovery of direct threats to the confidentiality, integrity, or availability of CJI.	10/1/2024	P1	Agency	Both	Both
AC-3	AC-3	ACCESS ENFORCEMENT	Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	Existing	P1	Agency	Both	Both
AC-3(14)	AC-3(14)	(14) ACCESS ENFORCEMENT | INDIVIDUAL ACCESS	Provide automated or manual processes to enable individuals to have access to elements of their personally identifiable information.	Existing	P1	Agency	Both	Both

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
AC-4	AC-4	INFORMATION FLOW ENFORCEMENT	Enforce approved authorizations for controlling the flow of information within the system and between connected systems by preventing CJI from being transmitted unencrypted across the public network, blocking outside traffic that claims to be from within the agency, and not passing any web requests to the public network that are not from agency controlled or internal boundary protection devices (e.g., proxies, gateways, firewalls, or routers).	Existing	P1	Agency	Both	Both
AC-5	AC-5	SEPARATION OF DUTIES	a. Identify and document separation of duties based on specific duties, operations, or information systems, as necessary, to mitigate risk to CJI; and	Existing	P1	Agency	Both	Both
		"	b. Define system access authorizations to support separation of duties.	Existing	P1	Agency	Both	Both
AC-6	AC-6	LEAST PRIVILEGE	Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.	Existing	P1	Agency	Both	Both
AC-6(1)	AC-6(1)	(1) LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS	Authorize access for personnel including, security administrators, system and network administrators, and other privileged users with access to system control, monitoring, or administration functions (e.g., system administrators, information security personnel, maintainers, system programmers, etc.) to:	Existing	P1	Agency	Both	Both
		"	(a) Established system accounts, configured access authorizations (i.e., permissions, privileges), set events to be audited, set intrusion detection parameters, and other security functions; and	Existing	P1	Agency	Both	Both
		"	(b) Security-relevant information in hardware, software, and firmware.	Existing	P1	Agency	Both	Both
AC-6(2)	AC-6(2)	(2) LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS	Require that users of system accounts (or roles) with access to privileged security functions or security-relevant information (e.g., audit logs), use non-privileged accounts or roles, when accessing nonsecurity functions.	Existing	P1	Agency	Both	Both
AC-6(5)	AC-6(5)	(5) LEAST PRIVILEGE | PRIVILEGED ACCOUNTS	Restrict privileged accounts on the system to privileged users.	Existing	P1	Agency	Both	Both
AC-6(7)	AC-6(7)	(7) LEAST PRIVILEGE | REVIEW OF USER PRIVILEGES	a. Reviews annually the privileges assigned to non-privileged and privileged users to validate the need for such privileges; and	Existing	P1	Agency	Both	Both
		"	b. Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs.	Existing	P1	Agency	Both	Both
AC-6(9)	AC-6(9)	(9) LEAST PRIVILEGE | LOG USE OF PRIVILEGED FUNCTIONS	Log the execution of privileged functions.	Existing	P1	Agency	Both	Both
AC-6(10)	AC-6(10)	(10) LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS	Prevent non-privileged users from executing privileged functions.	Existing	P1	Agency	Both	Both
AC-7	AC-7	UNSUCCESSFUL LOGON ATTEMPTS	a. Enforce a limit of five (5) consecutive invalid logon attempts by a user during a 15-minute time period; and	Existing	P3	Agency	Both	Both
		"	b. Automatically lock the account or node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.	Existing	P3	Agency	Both	Both
AC-8	AC-8	SYSTEM USE NOTIFICATION	a. Display a system use notification message to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that:	Existing	P2	Agency	Both	Both
		"	1. Users are accessing a restricted information system;	Existing	P2	Agency	Both	Both
		"	2. System usage may be monitored, recorded, and subject to audit;	Existing	P2	Agency	Both	Both

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
AC-8	AC-8	SYSTEM USE NOTIFICATION (continued)	3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and	Existing	P2	Agency	Both	Both
		"	4. Use of the system indicates consent to monitoring and recording;	Existing	P2	Agency	Both	Both
		"	b. Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system; and	Existing	P2	Agency	Both	Both
		"	c. For publicly accessible systems:	Existing	P2	Agency	Both	Both
		"	1. Display system use information consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines, before granting further access to the publicly accessible system;	Existing	P2	Agency	Both	Both
		"	2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and	Existing	P2	Agency	Both	Both
		"	3. Include a description of the authorized uses of the system.	Existing	P2	Agency	Both	Both
AC-11	AC-11	DEVICE LOCK	a. Prevent further access to the system by initiating a device lock after a maximum of 30 minutes of inactivity and requiring the user to initiate a device lock before leaving the system unattended.	Existing	P4	Agency	Both	Both
		"	NOTE: In the interest of safety, devices that are: (1) part of a criminal justice conveyance; or (2) used to perform dispatch functions and located within a physically secure location; or (3) terminals designated solely for the purpose of receiving alert notifications (i.e., receive only terminals or ROT) used within physically secure location facilities that remain staffed when in operation, are exempt from this requirement.	Existing	P4	Agency	Both	Both
		"	b. Retain the device lock until the user reestablishes access using established identification and authentication procedures.	Existing	P4	Agency	Both	Both
AC-11(1)	AC-11(1)	(1) DEVICE LOCK | PATTERN-HIDING DISPLAYS	Conceal, via the device lock, information previously visible on the display with a publicly viewable image.	Existing	P4	Agency	Both	Both
AC-12	AC-12	SESSION TERMINATION	Automatically terminate a user session after a user has been logged out.	Zero-cycle	P3	Agency	Both	Both
AC-14	AC-14	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION	a. Identify any specific user actions that can be performed on the system without identification or authentication consistent with organizational mission and business functions; and	Zero-cycle	P4	Agency	Both	Both
		"	b. Document and provide supporting rationale in the security plan for the system, user actions not requiring identification or authentication.	Zero-cycle	P4	Agency	Both	Both
AC-17	AC-17	REMOTE ACCESS	a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and	Existing	P1	Agency	Both	Both
		"	b. Authorize each type of remote access to the system prior to allowing such connections.	Existing	P1	Agency	Both	Both
AC-17(1)	AC-17(1)	(1) REMOTE ACCESS | MONITORING AND CONTROL	Employ automated mechanisms to monitor and control remote access methods.	Existing	P1	Agency	Both	Both
AC-17(2)	AC-17(2)	(2) REMOTE ACCESS | PROTECTION OF CONFIDENTIALITY AND INTEGRITY USING ENCRYPTION	Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.	Existing	P1	Agency	Both	Both
AC-17(3)	AC-17(3)	(3) REMOTE ACCESS | MANAGED ACCESS CONTROL POINTS	Route remote accesses through authorized and managed network access control points.	Existing	P1	Agency	Both	Both
AC-17(4)	AC-17(4)	(4) REMOTE ACCESS | PRIVILEGED COMMANDS AND ACCESS	(a) Authorize the execution of privileged commands and access to security-relevant information via remote access only in a format that provides assessable evidence and for the following needs: compelling operational needs; and	Existing	P1	Agency	Both	Both
		"	(b) Document the rationale for remote access in the security plan for the system.	Existing	P1	Agency	Both	Both

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
AC-18	AC-18	WIRELESS ACCESS	a. Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access; and	Existing	P2	Agency	Both	Both
		"	b. Authorize each type of wireless access to the system prior to allowing such connections.	Existing	P2	Agency	Both	Both
AC-18(1)	AC-18(1)	(1) WIRELESS ACCESS | AUTHENTICATION AND ENCRYPTION	Protect wireless access to the system using authentication of authorized users and agency-controlled devices, and encryption.	Existing	P2	Agency	Both	Both
AC-18(3)	AC-18(3)	(3) WIRELESS ACCESS | DISABLE WIRELESS NETWORKING	Disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment.	Existing	P2	Agency	Both	Both
AC-19	AC-19	ACCESS CONTROL FOR MOBILE DEVICES	a. Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas; and	Existing	P2	Agency	Both	Both
		"	b. Authorize the connection of mobile devices to organizational systems.	Existing	P2	Agency	Both	Both
AC-19(5)	AC-19(5)	(5) ACCESS CONTROL FOR MOBILE DEVICES | FULL DEVICE OR CONTAINER-BASED ENCRYPTION	Employ full-device encryption to protect the confidentiality and integrity of information on full- and limited-feature operating system mobile devices authorized to process, store, or transmit CJI.	Existing	P2	Agency	Both	Both
AC-20	AC-20	USE OF EXTERNAL SYSTEMS	a. Establish agency-level policies governing the use of external systems consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to:	Existing	P1	Agency	Both	Both
		"	1. Access the system from external systems; and	Existing	P1	Agency	Both	Both
		"	2. Process, store, or transmit organization-controlled information using external systems; or	Existing	P1	Agency	Both	Both
		"	b. Prohibit the use of personally-owned information systems including mobile devices (i.e., bring your own device [BYOD]) and publicly accessible systems for accessing, processing, storing, or transmitting CJI.	10/1/2024	P1	Agency	Both	Both
AC-20(1)	AC-20(1)	(1) USE OF EXTERNAL SYSTEMS | LIMITS ON AUTHORIZED USE	Permit authorized individuals to use an external system to access the system or to process, store, or transmit organization-controlled information only after:	Existing	P1	Agency	Both	Both
		"	(a) Verification of the implementation of controls on the external system as specified in the organization's security and privacy policies and security and privacy plans; or	Existing	P1	Agency	Both	Both
		"	(b) Retention of approved system connection or processing agreements with the organizational entity hosting the external system.	Existing	P1	Agency	Both	Both
AC-20(2)	AC-20(2)	(2) USE OF EXTERNAL SYSTEMS | PORTABLE STORAGE DEVICES — RESTRICTED USE	Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems.	Existing	P1	Agency	Both	Both
AC-21	AC-21	INFORMATION SHARING	a. Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions as defined in an executed information exchange agreement; and	Existing	P3	Agency	Both	Both
		"	b. Employ attribute-based access control (see AC-2(d)(3)) or manual processes as defined in information exchange agreements to assist users in making information sharing and collaboration decisions.	Existing	P3	Agency	Both	Both

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
AC-22	AC-22	PUBLICLY ACCESSIBLE CONTENT	a. Designate individuals authorized to make information publicly accessible;	Zero-cycle	P4	Agency	Both	Both
		"	b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information;	Zero-cycle	P4	Agency	Both	Both
		"	c. Review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included; and	Zero-cycle	P4	Agency	Both	Both
		"	d. Review the content on the publicly accessible system for nonpublic information quarterly and remove such information, if discovered.	Zero-cycle	P4	Agency	Both	Both

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy Section 5-6: 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.	Existing	Existing	Agency	Agency	Agency
		"	The original identifier between the requesting agency and the CSA/SIB/Channeler shall be the ORI, and other agency identifiers, such as user identification or personal identifier, an access device mnemonic, or the Internet Protocol (IP) address.	Existing	Existing	Agency	Agency	Agency
		"	Because the agency performing the transaction may not necessarily be the same as the agency requesting the transaction, the CSA/SIB/Channeler shall ensure that the ORI for each transaction can be traced, via audit trail, to the specific agency which is requesting the transaction.	Existing	Existing	Agency	Agency	Agency
		"	Agencies assigned a limited access ORI shall not use the full access ORI of another agency to conduct an inquiry transaction.	Existing	Existing	Agency	Agency	Agency
5.6: IA-1	5.6: IA-1	Policy and Procedures	a. Develop, document, and disseminate to authorized personnel:	Zero-cycle	P2	Agency	Agency	Agency
		"	1. Agency/Entity identification and authentication policy that:	Zero-cycle	P2	Agency	Agency	Agency
		"	(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Zero-cycle	P2	Agency	Agency	Agency
		"	(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and	Zero-cycle	P2	Agency	Agency	Agency
		"	2. Procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls;	Zero-cycle	P2	Agency	Agency	Agency
		"	b. Designate an individual with security responsibilities to manage the development, documentation, and dissemination of the identification and authentication policy and procedures; and	Zero-cycle	P2	Agency	Agency	Agency
		"	c. Review and update the current identification and authentication:	Zero-cycle	P2	Agency	Agency	Agency
		"	1. Policy annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI; and	Zero-cycle	P2	Agency	Agency	Agency
		"	2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.	Zero-cycle	P2	Agency	Agency	Agency
5.6: IA-2	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.	Existing	P1	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	P1	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	P1	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	P1	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	P1	Agency	Both	Both
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.	Zero-cycle	P2	Agency	Both	Both

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
5.6: IA-4	5.6: IA-4	Identifier Management	Manage system identifiers by:	Existing	P2	Agency	Both	Both
		"	a. Receiving authorization from organizational personnel with identifier management responsibilities to assign an individual, group, role, service, or device identifier;	Existing	P2	Agency	Both	Both
		"	b. Selecting an identifier that identifies an individual, group, role, service, or device;	Existing	P2	Agency	Both	Both
		"	c. Assigning the identifier to the intended individual, group, role, service, or device; and	Existing	P2	Agency	Both	Both
		"	d. Preventing reuse of identifiers for one (1) year.	Zero-cycle	P2	Agency	Both	Both
5.6: IA-4 (4)	5.6: IA-4 (4)	Identifier Management | Identify User Status	Manage individual identifiers by uniquely identifying each individual as agency or non-agency.	Zero-cycle	P2	Agency	Both	Both
5.6: IA-5	5.6: IA-5	Authenticator Management	Manage system authenticators by:	Existing	P1	Agency	Both	Both
		"	a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator;	Zero-cycle	P1	Agency	Both	Both
		"	b. Establishing initial authenticator content for any authenticators issued by the organization;	Existing	P1	Agency	Both	Both
		"	c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;	Zero-cycle	P1	Agency	Both	Both
		"	d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators;	Existing	P1	Agency	Both	Both
		"	e. Changing default authenticators prior to first use;	Existing	P1	Agency	Both	Both
		"	f. Changing or refreshing authenticators annually or when there is evidence of authenticator compromise;	Existing	P1	Agency	Both	Both
		"	g. Protecting authenticator content from unauthorized disclosure and modification;	Existing	P1	Agency	Both	Both
		"	h. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and	10/1/2024	P1	Agency	Both	Both
		"	i. Changing authenticators for group or role accounts when membership to those accounts changes.	10/1/2024	P1	Agency	Both	Both
		"	j. All credential service providers (CSPs) authenticating claimants at Authenticator Assurance Level 2 (AAL2) SHALL be assessed on the following criteria:	10/1/2024	P1			
		"	(1) Authentication SHALL occur by the use of either a multi-factor authenticator or a combination of two single-factor authenticators.	10/1/2024	P1	Agency	Both	Both
		"	(2) If the multi-factor authentication process uses a combination of two single-factor authenticators, then it SHALL include a Memorized Secret authenticator and a possession-based authenticator. (NIST 800-63B, Section	10/1/2024	P1	Agency	Both	Both
		"	(3) Cryptographic authenticators used at AAL2 SHALL use approved cryptography.	10/1/2024	P1	Agency	Both	Both
		"	(4) At least one authenticator used at AAL2 SHALL be replay resistant.	10/1/2024	P1	Agency	Both	Both
		"	(5) Communication between the claimant and verifier SHALL be via an authenticated protected channel.	10/1/2024	P1	Agency	Both	Both
		"	(6) Verifiers operated by government agencies at AAL2 SHALL be validated to meet the requirements of FIPS 140 Level 1.	10/1/2024	P1	Agency	Both	Both
		"	(7) Authenticators procured by government agencies SHALL be validated to meet the requirements of FIPS 140 Level 1.	10/1/2024	P1	Agency	Both	Both

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
		Authenticator Management (continued)	(8) If a device such as a smartphone is used in the authentication process, then the unlocking of that device (typically done using a PIN or biometric) SHALL NOT be considered one of the authentication factors.	10/1/2024	P1	Agency	Both	Both
		"	(9) If a biometric factor is used in authentication at AAL2, then the performance requirements stated in IA-5 m Biometric Requirements SHALL be	10/1/2024	P1	Agency	Both	Both
		"	(10) Reauthentication of the subscriber SHALL be repeated at least once per 12 hours during an extended usage session.	10/1/2024	P1	Agency	Both	Both
		"	(11) Reauthentication of the subscriber SHALL be repeated following any period of inactivity lasting 30 minutes or longer.	10/1/2024	P1	Agency	Both	Both
		"	(12) The CSP SHALL employ appropriately tailored security controls from the moderate baseline of security controls defined in the CJIS Security Policy.	10/1/2024	P1	Agency	Both	Both
		"	The CSP SHALL ensure that the minimum assurance-related controls for moderate-impact systems are satisfied.	10/1/2024	P1	Agency	Both	Both
		"	(13) The CSP SHALL comply with records retention policies in accordance with applicable laws and regulations.	10/1/2024	P1	Agency	Both	Both
		"	(14) If the CSP opts to retain records in the absence of any mandatory requirements, then the CSP SHALL conduct a risk management process, including assessments of privacy and security risks to determine how long records should be retained and SHALL inform subscribers of that retention policy.	10/1/2024	P1	Agency	Both	Both
		"	k. Privacy requirements that apply to all CSPs, verifiers, and RPs.	10/1/2024	P1			
		"	(1) The CSP SHALL employ appropriately tailored privacy controls from the CJIS Security Policy.	10/1/2024	P1	Agency	Both	Both
5.6: IA-5	5.6: IA-5	"	(2) If the CSP processes attributes for purposes other than identity proofing, authentication, or attribute assertions (collectively "identity service"), related fraud mitigation, or to comply with law or legal process, then the CSP SHALL implement measures to maintain predictability and manageability commensurate with the associated privacy risk.	10/1/2024	P1	Agency	Both	Both
		"	l. General requirements applicable to AAL2 authentication process.	10/1/2024	P1			
		"	(1) CSPs SHALL provide subscriber instructions on how to appropriately protect a physical authenticator against theft or loss.	10/1/2024	P1	Agency	Both	Both
		"	(2) The CSP SHALL provide a mechanism to revoke or suspend the authenticator immediately upon notification from subscriber that loss or theft of the authenticator is suspected.	10/1/2024	P1	Agency	Both	Both
		"	(3) If required by the authenticator type descriptions in IA-5(1), then the verifier SHALL implement controls to protect against online guessing attacks.	10/1/2024	P1	Agency	Both	Both
		"	(4) If required by the authenticator type descriptions in IA-5(1) and the description of a given authenticator does not specify otherwise, then the verifier SHALL limit consecutive failed authentication attempts on a single account to no more than 100.	10/1/2024	P1	Agency	Both	Both
		"	(5) If signed attestations are used, then they SHALL be signed using a digital signature that provides at least the minimum security strength specified in the latest revision of 112 bits as of the date of this publication.	10/1/2024	P1	Agency	Both	Both
		"	(6) If the verifier and CSP are separate entities (as shown by the dotted line in Figure 8 Digital Identity Model), then communications between the verifier and CSP SHALL occur through a mutually-authenticated secure channel (such as a client-authenticated TLS connection).	10/1/2024	P1	Agency	Both	Both
		"	(7) If the CSP provides the subscriber with a means to report loss, theft, or damage to an authenticator using a backup or alternate authenticator, then that authenticator SHALL be either a memorized secret or a physical authenticator.	10/1/2024	P1	Agency	Both	Both

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
		Authenticator Management (continued)	(8) If the CSP chooses to verify an address of record (i.e., email, telephone, postal) and suspend authenticator(s) reported to have been compromised, then...The suspension SHALL be reversible if the subscriber successfully authenticates to the CSP using a valid (i.e., not suspended) authenticator and requests reactivation of an authenticator suspended in this manner.	10/1/2024	P1	Agency	Both	Both
		"	(9) If and when an authenticator expires, it SHALL NOT be usable for authentication.	10/1/2024	P1	Agency	Both	Both
		"	(10) The CSP SHALL have a documented process to require subscribers to surrender or report the loss of any physical authenticator containing attribute certificates signed by the CSP as soon as practical after expiration or receipt of a renewed authenticator.	10/1/2024	P1	Agency	Both	Both
		"	(11) CSPs SHALL revoke the binding of authenticators immediately upon notification when an online identity ceases to exist (e.g., subscriber's death, discovery of a fraudulent subscriber), when requested by the subscriber, or when the CSP determines that the subscriber no longer meets its eligibility requirements.	10/1/2024	P1	Agency	Both	Both
		"	(12) The CSP SHALL have a documented process to require subscribers to surrender or report the loss of any physical authenticator containing certified attributes signed by the CSP within five (5) days after revocation or termination takes place.	10/1/2024	P1	Agency	Both	Both
		"	m. Biometric Requirements	10/1/2024	P1			
		"	(1) Biometrics SHALL be used only as part of multi-factor authentication with a physical authenticator (something you have).	10/1/2024	P1	Agency	Both	Both
5.6: IA-5	5.6: IA-5	"	(2) An authenticated protected channel between sensor (or an endpoint containing a sensor that resists sensor replacement) and verifier SHALL be established.	10/1/2024	P1	Agency	Both	Both
		"	(3) The sensor or endpoint SHALL be authenticated prior to capturing the biometric sample from the claimant.	10/1/2024	P1	Agency	Both	Both
		"	(4) The biometric system SHALL operate with an FMR [ISO/IEC 2382-37] of 1 in 1000 or better. This FMR SHALL be achieved under conditions of a conformant attack (i.e., zero-effort impostor attempt) as defined in [ISO/IEC 30107-1].	10/1/2024	P1	Agency	Both	Both
		"	(5) The biometric system SHALL allow no more than 5 consecutive failed authentication attempts or 10 consecutive failed attempts if PAD demonstrating at least 90% resistance to presentation attacks is implemented.	10/1/2024	P1	Agency	Both	Both
		"	(6) Once the limit on authentication failures has been reached, the biometric authenticator SHALL either:	10/1/2024	P1	Agency	Both	Both
		"	i. Impose a delay of at least 30 seconds before the next attempt, increasing exponentially with each successive attempt, or	10/1/2024	P1	Agency	Both	Both
		"	ii. disable the biometric user authentication and offer another factor (e.g., a different biometric modality or a PIN/Passcode if it is not already a required factor) if such an alternative method is already available.	10/1/2024	P1	Agency	Both	Both
		"	(7) The verifier SHALL make a determination of sensor and endpoint performance, integrity, and authenticity.	10/1/2024	P1	Agency	Both	Both
		"	(8) If biometric comparison is performed centrally, then use of the biometric as an authentication factor SHALL be limited to one or more specific devices that are identified using approved cryptography.	10/1/2024	P1	Agency	Both	Both
		"	(9) If biometric comparison is performed centrally, then a separate key SHALL be used for identifying the device.	10/1/2024	P1	Agency	Both	Both

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
		Authenticator Management (continued)	(10) If biometric comparison is performed centrally, then biometric revocation, referred to as biometric template protection in ISO/IEC 24745, SHALL be implemented.	10/1/2024	P1	Agency	Both	Both
		"	(11) If biometric comparison is performed centrally, all transmission of biometrics SHALL be over the authenticated protected channel.	10/1/2024	P1	Agency	Both	Both
		"	(12) Biometric samples and any biometric data derived from the biometric sample such as a probe produced through signal processing SHALL be zeroized immediately after any training or research data has been derived	10/1/2024	P1	Agency	Both	Both
		"	n. Authenticator binding refers to the establishment of an association between a specific authenticator and a subscriber's account, enabling the authenticator to be used — possibly in conjunction with other authenticators — to authenticate for that account.	10/1/2024	P1			
		"	(1) Authenticators SHALL be bound to subscriber accounts by either issuance by the CSP as part of enrollment or associating a subscriber-provided authenticator that is acceptable to the CSP.	10/1/2024	P1	Agency	Both	Both
		"	(2) Throughout the digital identity lifecycle, CSPs SHALL maintain a record of all authenticators that are or have been associated with each identity.	10/1/2024	P1	Agency	Both	Both
		"	(3) The CSP or verifier SHALL maintain the information required for throttling authentication attempts.	10/1/2024	P1	Agency	Both	Both
		"	(4) The CSP SHALL also verify the type of user-provided authenticator so verifiers can determine compliance with requirements at each AAL.	10/1/2024	P1	Agency	Both	Both
		"	(5) The record created by the CSP SHALL contain the date and time the authenticator was bound to the account.	10/1/2024	P1	Agency	Both	Both
5.6: IA-5	5.6: IA-5	"	(6) When any new authenticator is bound to a subscriber account, the CSP SHALL ensure that the binding protocol and the protocol for provisioning the associated key(s) are done at AAL2.	10/1/2024	P1	Agency	Both	Both
		"	(7) Protocols for key provisioning SHALL use authenticated protected channels or be performed in person to protect against man-in-the- middle attacks.	10/1/2024	P1	Agency	Both	Both
		"	(8) Binding of multi-factor authenticators SHALL require multi-factor authentication (or equivalent) at identity proofing.	10/1/2024	P1	Agency	Both	Both
		"	(9) At enrollment, the CSP SHALL bind at least one, and SHOULD bind at least two, physical (something you have) authenticators to the subscriber's online identity, in addition to a memorized secret or one or more biometrics.	10/1/2024	P1	Agency	Both	Both
		"	(10) At enrollment, authenticators at AAL2 and IAL2 SHALL be bound to the account.	10/1/2024	P1	Agency	Both	Both
		"	(11) If the subscriber is authenticated at AAL1, then the CSP SHALL NOT expose personal information, even if self-asserted, to the subscriber.	10/1/2024	P1	Agency	Both	Both
		"	(12) If enrollment and binding are being done remotely and cannot be completed in a single electronic transaction, then the applicant SHALL identify themselves in each new binding transaction by presenting a temporary secret which was either established during a prior transaction, or sent to the applicant's phone number, email address, or postal address of record.	10/1/2024	P1	Agency	Both	Both
		"	(13) If enrollment and binding are being done remotely and cannot be completed in a single electronic transaction, then long-term authenticator secrets are delivered to the applicant within a protected session.	10/1/2024	P1	Agency	Both	Both
		"	(14) If enrollment and binding are being done in person and cannot be completed in a single physical encounter, the applicant SHALL identify themselves in person by either using a secret as described in IA-5 n (12) above, or through use of a biometric that was recorded during a prior encounter.	10/1/2024	P1	Agency	Both	Both

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
5.6: IA-5	5.6: IA-5	Authenticator Management (continued)	(15) If enrollment and binding are being done in person and cannot be completed in a single physical encounter, temporary secrets SHALL NOT be reused.	10/1/2024	P1	Agency	Both	Both
		"	(16) If enrollment and binding are being done in person and cannot be completed in a single physical encounter and the CSP issues long-term authenticator secrets during a physical transaction, they SHALL be loaded locally onto a physical device that is issued in person to the applicant or delivered in a manner that confirms the address of record.	10/1/2024	P1	Agency	Both	Both
		"	(17) Before adding a new authenticator to a subscriber's account, the CSP SHALL first require the subscriber to authenticate at AAL2 (or a higher AAL) at which the new authenticator will be used.	10/1/2024	P1	Agency	Both	Both
		"	(18) If the subscriber's account has only one authentication factor bound to it, the CSP SHALL require the subscriber to authenticate at AAL1 in order to bind an additional authenticator of a different authentication factor.	10/1/2024	P1	Agency	Both	Both
		"	(19) If a subscriber loses all authenticators of a factor necessary to complete multi-factor authentication and has been identity proofed at IAL2, that subscriber SHALL repeat the identity proofing process described in IA-12.	10/1/2024	P1	Agency	Both	Both
		"	(20) If a subscriber loses all authenticators of a factor necessary to complete multi-factor authentication and has been identity proofed at IAL2 or IAL3, the CSP SHALL require the claimant to authenticate using an authenticator of the remaining factor, if any, to confirm binding to the existing identity.	10/1/2024	P1	Agency	Both	Both
		"	(21) If the CSP opts to allow binding of a new memorized secret with the use of two physical authenticators, then it requires entry of a confirmation code sent to an address of record.	10/1/2024	P1	Agency	Both	Both
		"	(22) If the CSP opts to allow binding of a new memorized secret with the use of two physical authenticators, then the confirmation code SHALL consist of at least 6 random alphanumeric characters generated by an approved random bit generator [SP 800-90Ar1].	10/1/2024	P1	Agency	Both	Both
		"	(23) If the CSP opts to allow binding of a new memorized secret with the use of two physical authenticators, then the confirmation code SHALL be valid for a maximum of 7 days but MAY be made valid up to 21 days via an exception process to accommodate addresses outside the direct reach of the U.S. Postal Service. Confirmation codes sent by means other than physical mail SHALL be valid for a maximum of 5 minutes.	10/1/2024	P1	Agency	Both	Both
		"	o. Session Management: The following requirements apply to applications where a session is maintained between the subscriber and relying party to allow multiple interactions without repeating the authentication event each time.	10/1/2024	P1			
		"	(1) Session Binding Requirements: A session occurs between the software that a subscriber is running — such as a browser, application, or operating system (i.e., the session subject) — and the RP or CSP that the subscriber is accessing (i.e., the session host).	10/1/2024	P1	Agency	Both	Both
		"	a. A session is maintained by a session secret which SHALL be shared between the subscriber's software and the service being accessed.	10/1/2024	P1	Agency	Both	Both
		"	b. The secret SHALL be presented directly by the subscriber's software or possession of the secret SHALL be proven using a cryptographic mechanism.	10/1/2024	P1	Agency	Both	Both
		"	c. The secret used for session binding SHALL be generated by the session host in direct response to an authentication event.	10/1/2024	P1	Agency	Both	Both
		"	d. A session SHALL NOT be considered at a higher AAL than the authentication event.	10/1/2024	P1	Agency	Both	Both

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
		Authenticator Management (continued)	e. Secrets used for session binding SHALL be generated by the session host during an interaction, typically immediately following authentication.	10/1/2024	P1	Agency	Both	Both
		"	f. Secrets used for session binding SHALL be generated by an approved random bit generator [SP 800-90Ar1].	10/1/2024	P1	Agency	Both	Both
		"	g. Secrets used for session binding SHALL contain at least 64 bits of entropy.	10/1/2024	P1	Agency	Both	Both
		"	h. Secrets used for session binding SHALL be erased or invalidated by the session subject when the subscriber logs out.	10/1/2024	P1	Agency	Both	Both
		"	i. Secrets used for session binding SHALL be sent to and received from the device using an authenticated protected channel.	10/1/2024	P1	Agency	Both	Both
		"	j. Secrets used for session binding SHALL time out and not be accepted after the times specified in IA-5 j (13) as appropriate for the AAL.	10/1/2024	P1	Agency	Both	Both
		"	k. Secrets used for session binding SHALL NOT be available to insecure communications between the host and subscriber's endpoint.	10/1/2024	P1	Agency	Both	Both
		"	l. Authenticated sessions SHALL NOT fall back to an insecure transport, such as from https to http, following authentication.	10/1/2024	P1	Agency	Both	Both
		"	m. URLs or POST content SHALL contain a session identifier that SHALL be verified by the RP to ensure that actions taken outside the session do not affect the protected session.	10/1/2024	P1	Agency	Both	Both
		"	n. Browser cookies SHALL be tagged to be accessible only on secure (HTTPS) sessions.	10/1/2024	P1	Agency	Both	Both
		"	o. Browser cookies SHALL be accessible to the minimum practical set of hostnames and paths.	10/1/2024	P1	Agency	Both	Both
5.6: IA-5	5.6: IA-5	"	p. Expiration of browser cookies SHALL NOT be depended upon to enforce session timeouts.	10/1/2024	P1	Agency	Both	Both
		"	q. The presence of an OAuth access token SHALL NOT be interpreted by the RP as presence of the subscriber, in the absence of other signals.	10/1/2024	P1	Agency	Both	Both
		"	(2) Reauthentication Requirements	10/1/2024	P1			
		"	a. Continuity of authenticated sessions SHALL be based upon the possession of a session secret issued by the verifier at the time of authentication and optionally refreshed during the session.	10/1/2024	P1	Agency	Both	Both
		"	b. Session secrets SHALL be non-persistent, i.e., they SHALL NOT be retained across a restart of the associated application or a reboot of the host device.	10/1/2024	P1	Agency	Both	Both
		"	c. Periodic reauthentication of sessions (at least every 12 hours per session) SHALL be performed to confirm the continued presence of the subscriber at an authenticated session.	10/1/2024	P1	Agency	Both	Both
		"	d. A session SHALL NOT be extended past the guidelines in IA-5 o (2) a – j based on presentation of the session secret alone.	10/1/2024	P1	Agency	Both	Both
		"	e. Prior to session expiration, the reauthentication time limit SHALL be extended by prompting the subscriber for the authentication factor(s) of a memorized secret or biometric.	10/1/2024	P1	Agency	Both	Both
		"	f. If federated authentication is being used, then since the CSP and RP often employ separate session management technologies, there SHALL NOT be any assumption of correlation between these sessions.	10/1/2024	P1	Agency	Both	Both
		"	g. An RP requiring reauthentication through a federation protocol SHALL — if possible within the protocol — specify the maximum (see IA-5 j (10)) acceptable authentication age to the CSP.	10/1/2024	P1	Agency	Both	Both

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
5.6: IA-5	5.6: IA-5	Authenticator Management (continued)	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	P1	Agency	Both	Both
		"	i. If federated authentication is being used, the CSP SHALL communicate the authentication event time to the RP to allow the RP to decide if the assertion is sufficient for reauthentication and to determine the time for the next reauthentication event.	10/1/2024	P1	Agency	Both	Both
5.6: IA-5 (1)	5.6: IA-5 (1)	Authenticator Management | Authenticator Types	(a) Memorized Secret Authenticators and Verifiers:	Existing	P1			
		"	(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;	Existing	P1	Agency	Both	Both
		"	(2) Require immediate selection of a new password upon account recovery;	10/1/2024	P1	Agency	Both	Both
		"	(3) Allow user selection of long passwords and passphrases, including spaces and all printable characters;	10/1/2024	P1	Agency	Both	Both
		"	(4) Employ automated tools to assist the user in selecting strong password authenticators;	10/1/2024	P1	Agency	Both	Both
		"	(5) Enforce the following composition and complexity rules: when agencies elect to follow basic password standards.	Existing	P1	Agency	Both	Both
		"	(a) Not be a proper name.	Existing	P1	Agency	Both	Both
		"	(b) Not be the same as the Userid.	Existing	P1	Agency	Both	Both
		"	(c) Expire within a maximum of 90 calendar days.	Existing	P1	Agency	Both	Both
		"	(d) Not be identical to the previous ten (10) passwords.	Existing	P1	Agency	Both	Both
		"	(e) Not be displayed when entered.	Existing	P1	Agency	Both	Both
		"	(6) If chosen by the subscriber, memorized secrets SHALL be at least 8 characters in length.	Existing	P1	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	P1	Agency	Both	Both
		"	(8) Truncation of the secret SHALL NOT be performed.	10/1/2024	P1	Agency	Both	Both
		"	(9) Memorized secret verifiers SHALL NOT permit the subscriber to store a “hint” that is accessible to an unauthenticated claimant.	Existing	P1	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.	Existing	P1	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.	Existing	P1	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.	Existing	P1	Agency	Both	Both
		"	(13) If a chosen secret is found in the list, the CSP or verifier SHALL provide the reason for rejection.	Existing	P1	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.	Existing	P1	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.	Existing	P1	Agency	Both	Both

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
5.6: IA-5 (1)	5.6: IA-5 (1)	Authenticator Management | Authenticator Types (continued)	(16) Verifiers SHALL force a change of memorized secret if there is evidence of compromise of the authenticator.	Existing	P1	Agency	Both	Both
		"	(17) The verifier SHALL use approved encryption when requesting memorized secrets in order to provide resistance to eavesdropping and MitM attacks.	Existing	P1	Agency	Both	Both
		"	(18) The verifier SHALL use an authenticated protected channel when requesting memorized secrets in order to provide resistance to eavesdropping and MitM attacks.	Existing	P1	Agency	Both	Both
		"	(19) Verifiers SHALL store memorized secrets in a form that is resistant to offline attacks.	Existing	P1	Agency	Both	Both
		"	(20) Memorized secrets SHALL be salted and hashed using a suitable one-way key derivation function.	Existing	P1	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.	Existing	P1	Agency	Both	Both
		"	(22) Both the salt value and the resulting hash SHALL be stored for each subscriber using a memorized secret authenticator	Existing	P1	Agency	Both	Both
		"	(23) If an additional iteration of a key derivation function using a salt value known only to the verifier is performed, then this secret salt value SHALL be generated with an approved random bit generator and of sufficient length.	10/1/2024	P1	Agency	Both	Both
		"	(24) If an additional iteration of a key derivation function using a salt value known only to the verifier is performed, then this secret salt value SHALL provide at least the minimum-security strength.	10/1/2024	P1	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	P1	Agency	Both	Both
		"	(b) Look-Up Secret Authenticators and Verifiers	10/1/2024	P1			
		"	(1) CSPs creating look-up secret authenticators SHALL use an approved random bit generator to generate the list of secrets.	10/1/2024	P1	Agency	Both	Both
		"	(2) Look-up secrets SHALL have at least 20 bits of entropy.	10/1/2024	P1	Agency	Both	Both
		"	(3) If look-up secrets are distributed online, then they SHALL be distributed over a secure channel in accordance with the post-enrollment binding requirements in IA-5 n 17 through 25.	10/1/2024	P1	Agency	Both	Both
		"	(4) Verifiers of look-up secrets SHALL prompt the claimant for the next secret from their authenticator or for a specific (e.g., numbered) secret.	10/1/2024	P1	Agency	Both	Both
		"	(5) A given secret from an authenticator SHALL be used successfully only once.	10/1/2024	P1	Agency	Both	Both
		"	(6) If a look-up secret is derived from a grid (bingo) card, then each cell of the grid SHALL be used only once.	10/1/2024	P1	Agency	Both	Both
		"	(7) Verifiers SHALL store look-up secrets in a form that is resistant to offline attacks.	10/1/2024	P1	Agency	Both	Both
		"	(8) If look-up secrets have at least 112 bits of entropy, then they SHALL be hashed with an approved one-way function	10/1/2024	P1	Agency	Both	Both
		"	(9) If look-up secrets have less than 112 bits of entropy, then they SHALL be salted and hashed using a suitable one-way key derivation function.	10/1/2024	P1	Agency	Both	Both
		"	(10) If look-up secrets have less than 112 bits of entropy, then the salt SHALL be at least 32 bits in length and be chosen arbitrarily to minimize salt value collisions among stored hashes.	10/1/2024	P1	Agency	Both	Both
		"	(11) If look-up secrets have less than 112 bits of entropy, then both the salt value and the resulting hash SHALL be stored for each look-up secret	10/1/2024	P1	Agency	Both	Both

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
5.6: IA-5 (1)	5.6: IA-5 (1)	Authenticator Management | Authenticator Types (continued)	(12) If look-up secrets that have less than 64 bits of entropy, then the verifier SHALL implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber's account.	10/1/2024	P1	Agency	Both	Both
		"	(13) The verifier SHALL use approved encryption when requesting look-up secrets in order to provide resistance to eavesdropping and MitM attacks.	10/1/2024	P1	Agency	Both	Both
		"	(14) The verifier SHALL use an authenticated protected channel when requesting look-up secrets in order to provide resistance to eavesdropping and MitM attacks.	10/1/2024	P1	Agency	Both	Both
		"	(c) Out-of-Band Authenticators and Verifiers	10/1/2024	P1			
		"	(1) The out-of-band authenticator SHALL establish a separate channel with the verifier in order to retrieve the out-of-band secret or authentication request.	10/1/2024	P1	Agency	Both	Both
		"	(2) Communication over the secondary channel SHALL be encrypted unless sent via the public switched telephone network (PSTN).	10/1/2024	P1	Agency	Both	Both
		"	(3) Methods that do not prove possession of a specific device, such as voice-over-IP (VOIP) or email, SHALL NOT be used for out-of-band authentication.	10/1/2024	P1	Agency	Both	Both
		"	(4) If PSTN is not being used for out-of-band communication, then the out-of-band authenticator SHALL uniquely authenticate itself by establishing an authenticated protected channel with the verifier.	10/1/2024	P1	Agency	Both	Both
		"	(5) If PSTN is not being used for out-of-band communication, then the out-of-band authenticator SHALL communicate with the verifier using approved cryptography.	10/1/2024	P1	Agency	Both	Both
		"	(6) If PSTN is not being used for out-of-band communication, then the key used to authenticate the out-of-band device SHALL be stored in suitably secure storage available to the authenticator application (e.g., keychain storage, TPM, TEE, secure element).	10/1/2024	P1	Agency	Both	Both
		"	(7) If the PSTN is used for out-of-band authentication and a secret is sent to the out-of-band device via the PSTN, then the out-of-band authenticator SHALL uniquely authenticate itself to a mobile telephone network using a SIM card or equivalent that uniquely identifies the device.	10/1/2024	P1	Agency	Both	Both
		"	(8) If the out-of-band authenticator sends an approval message over the secondary communication channel, it SHALL either accept transfer of a secret from the primary channel to be sent to the verifier via the secondary communications channel, or present a secret received via the secondary channel from the verifier and prompt the claimant to verify the consistency of that secret with the primary channel, prior to accepting a yes/no response from the claimant which it sends to the verifier.	10/1/2024	P1	Agency	Both	Both
		"	(9) The verifier SHALL NOT store the identifying key itself, but SHALL use a verification method (e.g., an approved hash function or proof of possession of the identifying key) to uniquely identify the authenticator.	10/1/2024	P1	Agency	Both	Both
		"	(10) Depending on the type of out-of-band authenticator, one of the following SHALL take place: transfer of a secret to the primary channel, transfer of a secret to the secondary channel, or verification of secrets by the claimant.	10/1/2024	P1	Agency	Both	Both
		"	(11) If the out-of-band authenticator operates by transferring the secret to the primary channel, then the verifier SHALL transmit a random secret to the out-of-band authenticator and then wait for the secret to be returned on the primary communication channel.	10/1/2024	P1	Agency	Both	Both

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
5.6: IA-5 (1)	5.6: IA-5 (1)	Authenticator Management | Authenticator Types (continued)	(12) If the out-of-band authenticator operates by transferring the secret to the secondary channel, then the verifier SHALL display a random authentication secret to the claimant via the primary channel and then wait for the secret to be returned on the secondary channel from the claimant's out-of- band authenticator.	10/1/2024	P1	Agency	Both	Both
		"	(13) If the out-of-band authenticator operates by verification of secrets by the claimant, then the verifier SHALL display a random authentication secret to the claimant via the primary channel, send the same secret to the out-of-band authenticator via the secondary channel for presentation to the claimant, and then wait for an approval (or disapproval) message via the secondary channel.	10/1/2024	P1	Agency	Both	Both
		"	(14) The authentication SHALL be considered invalid if not completed within 10 minutes.	10/1/2024	P1	Agency	Both	Both
		"	(15) Verifiers SHALL accept a given authentication secret only once during the validity period.	10/1/2024	P1	Agency	Both	Both
		"	(16) The verifier SHALL generate random authentication secrets with at least 20 bits of entropy.	10/1/2024	P1	Agency	Both	Both
		"	(17) The verifier SHALL generate random authentication secrets using an approved random bit generator.	10/1/2024	P1	Agency	Both	Both
		"	(18) If the authentication secret has less than 64 bits of entropy, the verifier SHALL implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber's account as described in IA-5 l (3) through (4).	10/1/2024	P1	Agency	Both	Both
		"	(19) If out-of-band verification is to be made using the PSTN, then the verifier SHALL verify that the pre-registered telephone number being used is associated with a specific physical device.	10/1/2024	P1	Agency	Both	Both
		"	(20) If out-of-band verification is to be made using the PSTN, then changing the pre-registered telephone number is considered to be the binding of a new authenticator and SHALL only occur as described in IA-5 n (17) through (25).	10/1/2024	P1	Agency	Both	Both
		"	(21) If PSTN is used for out-of-band authentication, then the CSP SHALL offer subscribers at least one alternate authenticator that is not RESTRICTED and can be used to authenticate at the required AAL.	10/1/2024	P1	Agency	Both	Both
		"	(22) If PSTN is used for out-of-band authentication, then the CSP SHALL Provide meaningful notice to subscribers regarding the security risks of the RESTRICTED authenticator and availability of alternative(s) that are not RESTRICTED.	10/1/2024	P1	Agency	Both	Both
		"	(23) If PSTN is used for out-of-band authentication, then the CSP SHALL address any additional risk to subscribers in its risk assessment.	10/1/2024	P1	Agency	Both	Both
		"	(24) If PSTN is used for out-of-band authentication, then the CSP SHALL develop a migration plan for the possibility that the RESTRICTED authenticator is no longer acceptable at some point in the future and include this migration plan in its digital identity acceptance statement.	10/1/2024	P1	Agency	Both	Both
		"	(d) OTP Authenticators and Verifiers	10/1/2024	P1			
		"	(1) The secret key and its algorithm SHALL provide at least the minimum security strength of 112 bits as of the date of this publication.	10/1/2024	P1	Agency	Both	Both
		"	(2) The nonce SHALL be of sufficient length to ensure that it is unique for each operation of the device over its lifetime.	10/1/2024	P1	Agency	Both	Both
		"	(3) OTP authenticators — particularly software-based OTP generators —SHALL NOT facilitate the cloning of the secret key onto multiple devices.	10/1/2024	P1	Agency	Both	Both

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
5.6: IA-5 (1)	5.6: IA-5 (1)	Authenticator Management | Authenticator Types (continued)	(4) The authenticator output SHALL have at least 6 decimal digits (approximately 20 bits) of entropy.	Existing	P1	Agency	Both	Both
		"	(5) If the nonce used to generate the authenticator output is based on a real-time clock, then the nonce SHALL be changed at least once every 2 minutes.	10/1/2024	P1	Agency	Both	Both
		"	(6) The OTP value associated with a given nonce SHALL be accepted only once.	Existing	P1	Agency	Both	Both
		"	(7) The symmetric keys used by authenticators are also present in the verifier and SHALL be strongly protected against compromise.	10/1/2024	P1	Agency	Both	Both
		"	(8) If a single-factor OTP authenticator is being associated with a subscriber account, then the verifier or associated CSP SHALL use approved cryptography to either generate and exchange or to obtain the secrets required to duplicate the authenticator output.	10/1/2024	P1	Agency	Both	Both
		"	(9) The verifier SHALL use approved encryption when collecting the OTP.	10/1/2024	P1	Agency	Both	Both
		"	(10) The verifier SHALL use an authenticated protected channel when collecting the OTP.	10/1/2024	P1	Agency	Both	Both
		"	(11) If a time-based OTP is used, it SHALL have a defined lifetime (recommended 30 seconds) that is determined by the expected clock drift — in either direction — of the authenticator over its lifetime, plus allowance for network delay and user entry of the OTP.	10/1/2024	P1	Agency	Both	Both
		"	(12) Verifiers SHALL accept a given time-based OTP only once during the validity period.	10/1/2024	P1	Agency	Both	Both
		"	(13) If the authenticator output has less than 64 bits of entropy, the verifier SHALL implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber's account as described in IA-5 l (3) through (4).	10/1/2024	P1	Agency	Both	Both
		"	(14) If the authenticator is multi-factor, then each use of the authenticator SHALL require the input of the additional factor.	10/1/2024	P1	Agency	Both	Both
		"	(15) If the authenticator is multi-factor and a memorized secret is used by the authenticator for activation, then that memorized secret SHALL be a randomly chosen numeric secret at least 6 decimal digits in length or other memorized secret meeting the requirements of IA-5 (1)(a).	10/1/2024	P1	Agency	Both	Both
		"	(16) If the authenticator is multi-factor, then use of a memorized secret for activation SHALL be rate limited as specified in IA-5 l (3) through (4).	10/1/2024	P1	Agency	Both	Both
		"	(17) If the authenticator is multi-factor and is activated by a biometric factor, then that factor SHALL meet the requirements of IA-5 m, including limits on the number of consecutive authentication failures.	10/1/2024	P1	Agency	Both	Both
		"	(18) If the authenticator is multi-factor, then the unencrypted key and activation secret or biometric sample — and any biometric data derived from the biometric sample such as a probe produced through signal processing — SHALL be zeroized immediately after an OTP has been generated.	10/1/2024	P1	Agency	Both	Both
		"	(19) If the authenticator is multi-factor, the verifier or CSP SHALL establish, via the authenticator source, that the authenticator is a multi-factor device.	10/1/2024	P1	Agency	Both	Both
		"	(20) In the absence of a trusted statement that it is a multi-factor device, the verifier SHALL treat the authenticator as single-factor, in accordance with IA-5 (1) (d) (1) through (13).	10/1/2024	P1	Agency	Both	Both
		"	(e) Cryptographic Authenticators and Verifiers (including single- and multi-factor cryptographic authenticators, both hardware- and software-based)	10/1/2024	P1			

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
5.6: IA-5 (1)	5.6: IA-5 (1)	Authenticator Management | Authenticator Types (continued)	(1) If the cryptographic authenticator is software based, the key SHALL be stored in suitably secure storage available to the authenticator application.	10/1/2024	P1	Agency	Both	Both
		"	(2) If the cryptographic authenticator is software based, the key SHALL be strongly protected against unauthorized disclosure by the use of access controls that limit access to the key to only those software components on the device requiring access.	10/1/2024	P1	Agency	Both	Both
		"	(3) If the cryptographic authenticator is software based, it SHALL NOT facilitate the cloning of the secret key onto multiple devices.	10/1/2024	P1	Agency	Both	Both
		"	(4) If the authenticator is single-factor and hardware-based, secret keys unique to the device SHALL NOT be exportable (i.e., cannot be removed from the device).	10/1/2024	P1	Agency	Both	Both
		"	(5) If the authenticator is hardware-based, the secret key and its algorithm SHALL provide at least the minimum-security length of 112 bits as of the date of this publication.	10/1/2024	P1	Agency	Both	Both
		"	(6) If the authenticator is hardware-based, the challenge nonce SHALL be at least 64 bits in length.	10/1/2024	P1	Agency	Both	Both
		"	(7) If the authenticator is hardware-based, approved cryptography SHALL be used.	10/1/2024	P1	Agency	Both	Both
		"	(8) Cryptographic keys stored by the verifier SHALL be protected against modification.	10/1/2024	P1	Agency	Both	Both
		"	(9) If symmetric keys are used, cryptographic keys stored by the verifier SHALL be protected against disclosure.	10/1/2024	P1	Agency	Both	Both
		"	(10) The challenge nonce SHALL be at least 64 bits in length.	10/1/2024	P1	Agency	Both	Both
		"	(11) The challenge nonce SHALL either be unique over the authenticator's lifetime or statistically unique (i.e., generated using an approved random bit generator).	10/1/2024	P1	Agency	Both	Both
		"	(12) The verification operation SHALL use approved cryptography.	10/1/2024	P1	Agency	Both	Both
		"	(13) If a multi-factor cryptographic software authenticator is being used, then each authentication requires the presentation of the activation factor.	10/1/2024	P1	Agency	Both	Both
		"	(14) If the authenticator is multi-factor, then any memorized secret used by the authenticator for activation SHALL be a randomly chosen numeric secret at least 6 decimal digits in length or other memorized secret meeting the requirements of IA-5 (1) (a).	10/1/2024	P1	Agency	Both	Both
		"	(15) If the authenticator is multi-factor, then use of a memorized secret for activation SHALL be rate limited as specified in IA-5 l (3) through (4).	10/1/2024	P1	Agency	Both	Both
		"	(16) If the authenticator is multi-factor and is activated by a biometric factor, then that factor SHALL meet the requirements of IA-5 m, including limits on the number of consecutive authentication failures.	10/1/2024	P1	Agency	Both	Both
		"	(17) If the authenticator is multi-factor, then the unencrypted key and activation secret or biometric sample — and any biometric data derived from the biometric sample such as a probe produced through signal processing — SHALL be zeroized immediately after an authentication transaction has taken place.	10/1/2024	P1	Agency	Both	Both
5.6: IA-5 (2)	5.6: IA-5 (2)	Authenticator Management | Public Key Based Authentication	(a) For public key-based authentication:	Existing	P1			
		"	(1) Enforce authorized access to the corresponding private key; and	Existing	P1	Agency	Both	Both
		"	(2) Map the authenticated identity to the account of the individual or group; and	Existing	P1	Agency	Both	Both
		"	(b) When public key infrastructure (PKI) is used:	Existing	P1	Agency	Both	Both

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
5.6: IA-5 (2)	5.6: IA-5 (2)	Authenticator Management | Public Key Based Authentication (continued)	(1) Validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; and	Existing	P1	Agency	Both	Both
		"	(2) Implement a local cache of revocation data to support path discovery and validation.	Existing	P1	Agency	Both	Both
5.6: IA-5 (6)	5.6: IA-5 (6)	Authenticator Management | Protection of Authenticators	Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access.	Existing	P1	Agency	Both	Both
5.6: IA-6	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.	Existing	P3	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.	Zero-cycle	P2	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.	Zero-cycle	P2	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.	Zero-cycle	P2	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	Zero-cycle	P2	Agency	Both	Both
		"	(b) Document and maintain a list of accepted external authenticators.	Zero-cycle	P2	Agency	Both	Both
5.6: IA-8 (4)	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.	Zero-cycle	P2	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.	Zero-cycle	P2	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;	Zero-cycle	P2	Agency	Both	Both
		"	b. Resolve user identities to a unique individual; and	Zero-cycle	P2	Agency	Both	Both
		"	c. Collect, validate, and verify identity evidence.	Zero-cycle	P2	Agency	Both	Both
5.6: IA-12 (2)	5.6: IA-12 (2)	Identity Proofing | Identity Evidence	Require evidence of individual identification be presented to the registration authority.	Zero-cycle	P2	Agency	Both	Both
5.6: IA-12 (3)	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.	Zero-cycle	P2	Agency	Both	Both
		"	b. Identity proofing SHALL NOT be performed to determine suitability or entitlement to gain access to services or benefits.	Zero-cycle	P2	Agency	Both	Both
		"	c. 1. Collection of PII SHALL be limited to the minimum necessary to resolve to a unique identity in a given context.	Zero-cycle	P2	Agency	Both	Both
		"	2. Collection of PII SHALL be limited to the minimum necessary to validate the existence of the claimed identity and associate the claimed identity with the applicant providing identity evidence for appropriate identity resolution, validation, and verification.	Zero-cycle	P2	Agency	Both	Both

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
5.6: IA-12 (3)	5.6: IA-12 (3)	Identity Proofing | Identity Evidence Validation and Verification (continued)	d. The CSP SHALL provide explicit notice to the applicant at the time of collection regarding the purpose for collecting and maintaining a record of the attributes necessary for identity proofing, including whether such attributes are voluntary or mandatory to complete the identity proofing process, and the consequences for not providing the attributes.	Zero-cycle	P2	Agency	Both	Both
		"	e. If CSPs process attributes for purposes other than identity proofing, authentication, or attribute assertions (collectively "identity service"), related fraud mitigation, or to comply with law or legal process, then CSPs SHALL implement measures to maintain predictability and manageability commensurate with the privacy risk arising from the additional processing.	Zero-cycle	P2	Agency	Both	Both
		"	f. If the CSP employs consent as part of its measures to maintain predictability and manageability, …then it SHALL NOT make consent for the additional processing a condition of the identity service.	Zero-cycle	P2	Agency	Both	Both
		"	g. The CSP SHALL provide mechanisms for redress of applicant complaints or problems arising from the identity proofing.	Zero-cycle	P2	Agency	Both	Both
		"	These [redress] mechanisms SHALL be easy for applicants to find and use.	Zero-cycle	P2	Agency	Both	Both
		"	h. The CSP SHALL assess the [redress] mechanisms for their efficacy in achieving resolution of complaints or problems.	Zero-cycle	P2	Agency	Both	Both
		"	i. The identity proofing and enrollment processes SHALL be performed according to an applicable written policy or *practice statement* that specifies the particular steps taken to verify identities.	Zero-cycle	P2	Agency	Both	Both
		"	j. The *practice statement* SHALL include control information detailing how the CSP handles proofing errors that result in an applicant not being successfully enrolled.	Zero-cycle	P2	Agency	Both	Both
		"	k. The CSP SHALL maintain a record, including audit logs, of all steps taken to verify the identity of the applicant as long as the identity exists in the information system.	Zero-cycle	P2	Agency	Both	Both
		"	l. The CSP SHALL record the types of identity evidence presented in the proofing process.	Zero-cycle	P2	Agency	Both	Both
		"	m. The CSP SHALL conduct a risk management process, including assessments of privacy and security risks to determine:	Zero-cycle	P2	Agency	Both	Both
		"	1. Any steps that it will take to verify the identity of the applicant beyond any mandatory requirements specified herein;	Zero-cycle	P2	Agency	Both	Both
		"	2. The PII, including any biometrics, images, scans, or other copies of the identity evidence that the CSP will maintain as a record of identity proofing (Note: Specific federal requirements may apply); and	Zero-cycle	P2	Agency	Both	Both
		"	3. The schedule of retention for these records (Note: CSPs may be subject to specific retention policies in accordance with applicable laws, regulations, or policies, including any National Archives and Records Administration (NARA) records retention schedules that may apply).	Zero-cycle	P2	Agency	Both	Both
		"	n. All PII collected as part of the enrollment process SHALL be protected to ensure confidentiality, integrity, and attribution of the information source.	Zero-cycle	P2	Agency	Both	Both
		"	o. "The entire proofing transaction, including transactions that involve a third party, SHALL occur over authenticated protected channels. "	Zero-cycle	P2	Agency	Both	Both
		"	p. "If the CSP uses fraud mitigation measures, then the CSP SHALL conduct a privacy risk assessment for these mitigation measures. "	Zero-cycle	P2	Agency	Both	Both

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
		Identity Proofing | Identity Evidence Validation and Verification (continued)	Such assessments SHALL include any privacy risk mitigations (e.g., risk acceptance or transfer, limited retention, use limitations, notice) or other technological mitigations (e.g., cryptography), and be documented per requirement IA-12(3) k – m above.	Zero-cycle	P2	Agency	Both	Both
		"	q. In the event a CSP ceases to conduct identity proofing and enrollment processes, then the CSP SHALL be responsible for fully disposing of or destroying any sensitive data including PII, or its protection from unauthorized access for the duration of retention.	Zero-cycle	P2	Agency	Both	Both
		"	r. Regardless of whether the CSP is a federal agency or non- federal entity, the following requirements apply to the federal agency offering or using the proofing service:	Zero-cycle	P2	Agency	Both	Both
		"	1. The agency SHALL consult with their Senior Agency Official for Privacy (SAOP) to conduct an analysis determining whether the collection of PII to conduct identity proofing triggers Privacy Act requirements.	Zero-cycle	P2	Agency	Both	Both
		"	2. The agency SHALL publish a System of Records Notice (SORN) to cover such collection, as applicable.	Zero-cycle	P2	Agency	Both	Both
		"	3. The agency SHALL consult with their SAOP to conduct an analysis determining whether the collection of PII to conduct identity proofing triggers E-Government Act of 2002 requirements.	Zero-cycle	P2	Agency	Both	Both
		"	4. The agency SHALL publish a Privacy Impact Assessment (PIA) to cover such collection, as applicable.	Zero-cycle	P2	Agency	Both	Both
		"	s. An enrollment code SHALL be comprised of one of the following:	Zero-cycle	P2	Agency	Both	Both
5.6: IA-12 (3)	5.6: IA-12 (3)	"	1. Minimally, a random six character alphanumeric or equivalent entropy. For example, a code generated using an approved random number generator or a serial number for a physical hardware authenticator; OR	Zero-cycle	P2	Agency	Both	Both
		"	2. A machine-readable optical label, such as a QR Code, that contains data of similar or higher entropy as a random six character alphanumeric.	Zero-cycle	P2	Agency	Both	Both
		"	t. Training requirements for personnel validating evidence SHALL be based on the policies, guidelines, or requirements of the CSP or RP.	Zero-cycle	P2	Agency	Both	Both
		"	u. This criterion applies to CSPs that provide identity proofing and enrollment services to minors (under the age of 18):	Zero-cycle	P2	Agency	Both	Both
		"	If the CSP provides identity proofing and enrollment services to minors (under the age of 18), then…the CSP SHALL give special consideration to the legal restrictions of interacting with minors unable to meet the evidence requirements of identity proofing [to ensure compliance with the Children's Online Privacy Protection Act of 1998 (COPPA), and other laws, as applicable]. "	Zero-cycle	P2	Agency	Both	Both
		"	Requirements v and w apply to the collection of biometric characteristics for in-person (physical or supervised remote) identity proofing and are mandatory at IAL3. These criteria also apply to CSPs that optionally choose to collect biometric characteristics through in-person identity-proofing identity proofing and enrollment at IAL2.					
		"	v. The CSP SHALL have the operator view the biometric source (e.g., fingers, face) for presence of non-natural materials and perform such inspections as part of the proofing process.	Zero-cycle	P2	Agency	Both	Both
		"	w. The CSP SHALL collect biometrics in such a way that ensures that the biometric is collected from the applicant, and not another subject. All biometric performance requirements in IA-5 m (1) through (12) apply.	Zero-cycle	P2	Agency	Both	Both
		"	x. The CSP SHALL support in-person or remote identity proofing, or both.	Zero-cycle	P2	Agency	Both	Both
		"	y. The CSP SHALL collect the following from the applicant:	Zero-cycle	P2	Agency	Both	Both

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
		Identity Proofing | Identity Evidence Validation and Verification (continued)	1. One piece of SUPERIOR or STRONG evidence if the evidence's issuing source, during its identity proofing event, confirmed the claimed identity by collecting two or more forms of SUPERIOR or STRONG evidence and the CSP validates the evidence directly with the issuing source; OR	Zero-cycle	P2	Agency	Both	Both
		"	2. Two pieces of STRONG evidence; OR	Zero-cycle	P2	Agency	Both	Both
		"	3. One piece of STRONG evidence plus two pieces of FAIR evidence	Zero-cycle	P2	Agency	Both	Both
		"	z. The CSP SHALL validate each piece of evidence with a process that can achieve the same strength as the evidence presented (see 'z' above). For example, if two forms of STRONG identity evidence are presented, each piece of evidence will be validated at a strength of STRONG.	Zero-cycle	P2	Agency	Both	Both
		"	aa. The CSP SHALL verify identity evidence as follows:	Zero-cycle	P2	Agency	Both	Both
		"	At a minimum, the applicant's binding to identity evidence must be verified by a process that is able to achieve a strength of STRONG.	Zero-cycle	P2	Agency	Both	Both
		"	bb. For IAL2 remote proofing: The collection of biometric characteristics for physical or biometric comparison of the applicant to the strongest piece of identity evidence provided to support the claimed identity performed remotely SHALL adhere to all requirements as specified in IA-5 m.	Zero-cycle	P2	Agency	Both	Both
		"	cc. Knowledge-based verification (KBV) SHALL NOT be used for in-person (physical or supervised remote) identity verification.	Zero-cycle	P2	Agency	Both	Both
		"	dd. The CSP SHALL employ appropriately tailored security controls, to include control enhancements, from the moderate or high baseline of security controls defined in the CJIS Security Policy.	Zero-cycle	P2	Agency	Both	Both
		"	The CSP SHALL ensure that the minimum assurance-related controls for moderate-impact systems are satisfied.	Zero-cycle	P2	Agency	Both	Both
5.6: IA-12 (3)	5.6: IA-12 (3)	"	ee. Supervised Remote Identity Proofing: Supervised remote identity proofing is intended to provide controls for comparable levels of confidence and security to in-person IAL3 identity proofing for identity proofing processes that are performed remotely. Supervised remote identity proofing is optional for CSPs; that is, if a CSP chooses to use supervised remote identity proofing, then the following requirements, (1) through (8), would apply. It should be noted that the term "supervised remote identity proofing" has specialized meaning and is used only to refer to the specialized equipment and the following control requirements, (1) through (8). In addition to those requirements presented in this document, as well as the applicable identity validation and verification requirements, CSPs that provide supervised remote identity proofing services must demonstrate conformance with the requirements contained in this section. The following requirements for supervised remote proofing apply specifically to IAL3. If the equipment/facilities used for supervised remote proofing are used for IAL2 identity proofing, the following requirements, (1) through (8), for supervised remote proofing do not apply. In this case, the requirements for conventional remote identity proofing are applicable.	Zero-cycle	P2	Agency	Both	Both
		"	(1) Supervised remote identity proofing and enrollment transactions SHALL meet the following requirements, in addition to the IAL3 validation and verification requirements specified in Section 4.6 .	Zero-cycle	P2	Agency	Both	Both
		"	(2) The CSP SHALL monitor the entire identity proofing session, from which the applicant SHALL NOT depart — for example, by a continuous high-resolution video transmission of the applicant.	Zero-cycle	P2	Agency	Both	Both
		"	(3) The CSP SHALL have a live operator participate remotely with the applicant for the entirety of the identity proofing session.	Zero-cycle	P2	Agency	Both	Both

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
		Identity Proofing | Identity Evidence Validation and Verification (continued)	(4) The CSP SHALL require all actions taken by the applicant during the identity proofing session to be clearly visible to the remote operator.	Zero-cycle	P2	Agency	Both	Both
		"	(5) The CSP SHALL require that all digital validation of evidence (e.g., via chip or wireless technologies) be performed by integrated scanners and sensors.	Zero-cycle	P2	Agency	Both	Both
		"	(6) The CSP SHALL require operators to have undergone a training program to detect potential fraud and to properly perform a supervised remote proofing session.	Zero-cycle	P2	Agency	Both	Both
		"	(7) The CSP SHALL employ physical tamper detection and resistance features appropriate for the environment in which it is located.	Zero-cycle	P2	Agency	Both	Both
		"	(8) The CSP SHALL ensure that all communications occur over a mutually authenticated protected channel.	Zero-cycle	P2	Agency	Both	Both
		"	ff. Trusted Referee: The use of trusted referees is optional for CSPs; that is, if a CSP chooses to use trusted referees for identity proofing and enrollment, then the following requirements, (1) through (3) would apply. The use of trusted referees is intended to assist in the identity proofing and enrollment for populations that are unable to meet IAL2 identity proofing requirements, or otherwise would be challenged to perform identity proofing and enrollment process requirements. Such populations may include, but are not limited to:	Zero-cycle	P2	Agency	Both	Both
5.6: IA-12 (3)	5.6: IA-12 (3)	"	· disabled individuals;	Zero-cycle	P2	Agency	Both	Both
		"	· elderly individuals;	Zero-cycle	P2	Agency	Both	Both
		"	· homeless individuals,	Zero-cycle	P2	Agency	Both	Both
		"	· individuals with little or no access to online services or computing devices;	Zero-cycle	P2	Agency	Both	Both
		"	· unbanked and individuals with little or no credit history;	Zero-cycle	P2	Agency	Both	Both
		"	· victims of identity theft;	Zero-cycle	P2	Agency	Both	Both
		"	· children under 18; and	Zero-cycle	P2	Agency	Both	Both
		"	· immigrants.	Zero-cycle	P2	Agency	Both	Both
		"	In addition to those requirements presented in the General section of this document, as well as the applicable IAL requirements, CSPs that use trusted referees in their identity proofing services must demonstrate conformance with the requirements contained in this section.					
		"	(1) If the CSP uses trusted referees, then…The CSP SHALL establish written policy and procedures as to how a trusted referee is determined and the lifecycle by which the trusted referee retains their status as a valid referee, to include any restrictions, as well as any revocation and suspension requirements.	Zero-cycle	P2	Agency	Both	Both
		"	(2) If the CSP uses trusted referees, then…The CSP SHALL proof the trusted referee at the same IAL as the applicant proofing.	Zero-cycle	P2	Agency	Both	Both
		"	(3) If the CSP uses trusted referees, then…The CSP SHALL determine the minimum evidence required to bind the relationship between the trusted referee and the applicant.	Zero-cycle	P2	Agency	Both	Both

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
5.6: IA-12 (5)	5.6: IA-12 (5)	(5) Identity Proofing | Address Confirmation	a. Require that a registration code or notice of proofing be delivered through an out-of-band channel to verify the users address (physical or digital) of record.	Zero-cycle	P2	Agency	Both	Both
		"	b. The CSP SHALL confirm address of record.	Zero-cycle	P2	Agency	Both	Both
		"	c. Valid records to confirm address SHALL be issuing source(s) or authoritative source(s).	Zero-cycle	P2	Agency	Both	Both
		"	Self-asserted address data that has not been confirmed in records SHALL NOT be used for confirmation.	Zero-cycle	P2	Agency	Both	Both
		"	d. Note that IAL2-7 applies only to in-person proofing at IAL2.	Zero-cycle	P2	Agency	Both	Both
		"	If the CSP performs in-person proofing for IAL2 and provides an enrollment code directly to the subscriber for binding to an authenticator at a later time, then the enrollment code…SHALL be valid for a maximum of seven (7) days.	Zero-cycle	P2	Agency	Both	Both
		"	e. For remote identity proofing at IAL2:	Zero-cycle	P2	Agency	Both	Both
		"	The CSP SHALL send an enrollment code to a confirmed address of record for the applicant.	Zero-cycle	P2	Agency	Both	Both
		"	f. For remote identity proofing at IAL2:	Zero-cycle	P2	Agency	Both	Both
		"	The applicant SHALL present a valid enrollment code to complete the identity proofing process.	Zero-cycle	P2	Agency	Both	Both
		"	g. Note that the following enrollment code validity periods apply to enrollment codes sent to confirmed addresses of record for IAL2 remote in-person proofing only.	Zero-cycle	P2	Agency	Both	Both
		"	Enrollment codes shall have the following maximum validities:	Zero-cycle	P2	Agency	Both	Both
		"	i. 10 days, when sent to a postal address of record within the contiguous United States;	Zero-cycle	P2	Agency	Both	Both
		"	ii. 30 days, when sent to a postal address of record outside the contiguous United States;	Zero-cycle	P2	Agency	Both	Both
		"	iii. 10 minutes, when sent to a telephone of record (SMS or voice);	Zero-cycle	P2	Agency	Both	Both
		"	iv. 24 hours, when sent to an email address of record.	Zero-cycle	P2	Agency	Both	Both
		"	h. If the enrollment code sent to the confirmed address of record as part of the remote identity proofing process at IAL2 is also intended to be an authentication factor, then…it SHALL be reset upon first use.	Zero-cycle	P2	Agency	Both	Both
		"	i. If the CSP performs remote proofing at IAL2 and optionally sends notification of proofing in addition to sending the required enrollment code, then…The CSP SHALL ensure the enrollment code and notification of proofing are sent to different addresses of record.	Zero-cycle	P2	Agency	Both	Both

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy Section 5-7: Configuration Management								
	CM-1	POLICY AND PROCEDURES	Develop, document, and disseminate to organizational personnel with configuration management responsibilities:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. Agency-level configuration management policy that:	Zero-cycle	P2	TBD	TBD	TBD
		"	(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Zero-cycle	P2	TBD	TBD	TBD
		"	(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and	Zero-cycle	P2	TBD	TBD	TBD
		"	2. Procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls;	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Designate organizational personnel with information security responsibilities to manage the development, documentation, and dissemination of the configuration management policy and procedures; and	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Review and update the current configuration management:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. Policy annually and following any hardware or software changes to systems which process, store, or transmit CJI; and	Zero-cycle	P2	TBD	TBD	TBD
		"	2. Procedures annually and following any hardware or software changes to systems which process, store, or transmit CJI.	Zero-cycle	P2	TBD	TBD	TBD
	CM-2	BASELINE CONFIGURATION	a. Develop, document, and maintain under configuration control, a current baseline configuration of the system;	10/1/2024	P1	TBD	TBD	TBD
5.7.1.2		"	b. Develop, document, and maintain a current and complete topological drawing depicting the interconnectivity of the agency network to criminal justice information systems and services; and	Existing	P1	Agency	Both	Both
		"	c. Review and update the baseline configuration and topological drawing of the system:	Existing	P1	Agency	Both	Both
		"	1. At least annually;	Existing	P1	Agency	Both	Both
		"	2. When required due to security-relevant changes to the system and/or security incidents occur; and	Existing	P1	Agency	Both	Both
		"	3. When system components are installed or upgraded.	Existing	P1	Agency	Both	Both
	CM-2(2)	(2) BASELINE CONFIGURATION | AUTOMATION SUPPORT FOR ACCURACY AND CURRENCY	Maintain the currency, completeness, accuracy, and availability of the baseline configuration of the system using automated mechanisms such as configuration management tools, hardware, software, firmware inventory tools, and network management tools.	10/1/2024	P1	TBD	TBD	TBD
	CM-2(3)	(3) BASELINE CONFIGURATION | RETENTION OF PREVIOUS CONFIGURATIONS	Retain at least one (1) ~~of~~ previous version~~s~~ of baseline configurations of the system to support rollback.	10/1/2024	P1	TBD	TBD	TBD
	CM-2(7)	(7) BASELINE CONFIGURATION | CONFIGURE SYSTEMS AND COMPONENTS FOR HIGH-RISK AREAS	a. Issue devices (e.g., mobile devices) with CJISSECPOL compliant configurations to individuals traveling to locations that the organization deems to be of significant risk; and	10/1/2024	P1	TBD	TBD	TBD
5.13.1.2.1		"	b. Apply the following controls to the systems or components when the individuals return from travel: examine the device for signs of physical tampering, purge and reimage disk drives and/or devices as required, and ensure all security controls are in place and functional	Existing	P1	Agency	Agency	Agency
	CM-3	CONFIGURATION CHANGE CONTROL	a. Determine and document the types of changes to the system that are configuration-controlled;	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses;	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Document configuration change decisions associated with the system;	Zero-cycle	P2	TBD	TBD	TBD

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
	CM-3	CONFIGURATION CHANGE CONTROL (continued)	d. Implement approved configuration-controlled changes to the system;	Zero-cycle	P2	TBD	TBD	TBD
		"	e. Retain records of configuration-controlled changes to the system for two (2) years;	Zero-cycle	P2	TBD	TBD	TBD
		"	f. Monitor and review activities associated with configuration-controlled changes to the system; and	Zero-cycle	P2	TBD	TBD	TBD
		"	g. Coordinate and provide oversight for configuration change control activities through personnel with configuration management responsibilities, a Configuration Control Board, or Change Advisory Board that convenes regularly or when hardware or software changes (i.e., updates, upgrades, replacements, etc.) to the information system are required.	Zero-cycle	P2	TBD	TBD	TBD
	CM-3(2)	(2) CONFIGURATION CHANGE CONTROL | TESTING, VALIDATION, AND DOCUMENTATION OF CHANGES	Test, validate, and document changes to the system before finalizing the implementation of the changes.	Zero-cycle	P2	TBD	TBD	TBD
	CM-3(4)	(4) CONFIGURATION CHANGE CONTROL | SECURITY AND PRIVACY REPRESENTATIVES	Require organizational personnel with information security and privacy responsibilities to be members of the Configuration Control Board or Change Advisory Board.	Zero-cycle	P2	TBD	TBD	TBD
	CM-4	IMPACT ANALYSES	Analyze changes to the system to determine potential security and privacy impacts prior to change implementation.	Zero-cycle	P3	TBD	TBD	TBD
	CM-4(2)	(2) IMPACT ANALYSES | VERIFICATION OF CONTROLS	After system changes, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security and privacy requirements for the system.	Zero-cycle	P3	TBD	TBD	TBD
5.7.2	CM-5	ACCESS RESTRICTIONS FOR CHANGE	Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.	Existing	P1	Agency	Both	Both
	CM-6	CONFIGURATION SETTINGS	a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using established best practices and guidelines such as Defense Information Systems Agency (DISA) Secure Technical Implementation Guidelines (STIGs), Center for Internet Security (CIS) Benchmarks, or Federal Information Processing Standards;	10/1/2024	P1	TBD	TBD	TBD
		"	b. Implement the configuration settings;	10/1/2024	P1	TBD	TBD	TBD
		"	c. Identify, document, and approve any deviations from established configuration settings for system components that store, process, or transmit CJI based on operational requirements; and	10/1/2024	P1	TBD	TBD	TBD
		"	d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.	10/1/2024	P1	TBD	TBD	TBD
5.7.1.1	CM-7	LEAST FUNCTIONALITY	a. Configure the system to provide only essential capabilities to meet operational requirements; and	10/1/2024	P1	TBD	TBD	TBD
		"	b. Prohibit or restrict the use of specified functions, ports, protocols, software, and/or services: which are not required.	Existing	P1	Agency	Both	Both
	CM-7(1)	(1) LEAST FUNCTIONALITY | PERIODIC REVIEW	a. Review the system annually, as the system changes, or incidents occur to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services; and	Existing	P1	Agency	Both	Both
		"	b. Disable or remove functions, ports, protocols, software, and/or services within the system deemed to be unnecessary and/or unsecure.	10/1/2024	P1	TBD	TBD	TBD
	CM-7(2)	(2) LEAST FUNCTIONALITY | PREVENT PROGRAM EXECUTION	Prevent program execution in accordance with rules of behavior and/or rules authorizing the terms and conditions of software program usage.	10/1/2024	P1	TBD	TBD	TBD

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
	CM-7(5)	(5) LEAST FUNCTIONALITY | AUTHORIZED SOFTWARE — ALLOW-BY-EXCEPTION	a. Identify software programs authorized to execute on the system;	10/1/2024	P1	TBD	TBD	TBD
		"	b. Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system; and	10/1/2024	P1	TBD	TBD	TBD
		"	c. Review and update the list of authorized software programs annually.	10/1/2024	P1	TBD	TBD	TBD
	CM-8	SYSTEM COMPONENT INVENTORY	a. Develop and document an inventory of system components that:	10/1/2024	P1	TBD	TBD	TBD
		"	1. Accurately reflects the system;	10/1/2024	P1	TBD	TBD	TBD
		"	2. Includes all components within the system;	10/1/2024	P1	TBD	TBD	TBD
		"	3. Does not include duplicate accounting of components or components assigned to any other system;	10/1/2024	P1	TBD	TBD	TBD
		"	4. Is at the level of granularity deemed necessary for tracking and reporting; and	10/1/2024	P1	TBD	TBD	TBD
		"	5. Includes the following minimum information to achieve system component accountability: date of installation, model, serial number, manufacturer, supplier information, component type, software owner, software version number, software license information, and hardware and physical location; and	10/1/2024	P1	TBD	TBD	TBD
		"	b. Review and update the system component inventory annually.	10/1/2024	P1	TBD	TBD	TBD
	CM-8(1)	(1) SYSTEM COMPONENT INVENTORY | UPDATES DURING INSTALLATION AND REMOVAL	Update the inventory of system components as part of component installations, removals, and system updates.	10/1/2024	P1	TBD	TBD	TBD
	CM-8(3)	(3) SYSTEM COMPONENT INVENTORY | AUTOMATED UNAUTHORIZED COMPONENT DETECTION	a. Detect the presence of unauthorized hardware, software, and firmware components within the system using automated mechanisms continuously or at least weekly; and	10/1/2024	P1	TBD	TBD	TBD
		"	b. Take the following actions when unauthorized components are detected: disable or isolate the unauthorized components and notify organizational personnel with security responsibilities.	10/1/2024	P1	TBD	TBD	TBD
	CM-9	CONFIGURATION MANAGEMENT PLAN	Develop, document, and implement a configuration management plan for the system that:	Zero-cycle	P2	TBD	TBD	TBD
		"	a. Addresses roles, responsibilities, and configuration management processes and procedures;	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Defines the configuration items for the system and places the configuration items under configuration management;	Zero-cycle	P2	TBD	TBD	TBD
		"	d. Is reviewed and approved by organizational personnel with information security responsibilities and organizational personnel with configuration management responsibilities; and	Zero-cycle	P2	TBD	TBD	TBD
		"	e. Protects the configuration management plan from unauthorized disclosure and modification.	Zero-cycle	P2	TBD	TBD	TBD
	CM-10	SOFTWARE USAGE RESTRICTIONS	a. Use software and associated documentation in accordance with contract agreements and copyright laws;	Zero-cycle	P3	TBD	TBD	TBD
		"	b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and	Zero-cycle	P3	TBD	TBD	TBD
		"	c. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.	Zero-cycle	P3	TBD	TBD	TBD

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
	CM-11	*USER-INSTALLED SOFTWARE*	*a. Establish agency-level policies governing the installation of software by users;*	Zero-cycle	P2	TBD	TBD	TBD
		"	*b. Enforce software installation policies through automated methods; and*	Zero-cycle	P2	TBD	TBD	TBD
		"	*c. Monitor policy compliance through automated methods at least weekly.*	Zero-cycle	P2	TBD	TBD	TBD
	CM-12	*INFORMATION LOCATION*	*a. Identify and document the location of CJI and the specific system components on which the information is processed, ~~and~~ stored, or transmitted;*	Zero-cycle	P2	TBD	TBD	TBD
		"	*b. Identify and document the users who have access to the system and system components where the information is processed and stored; and*	Zero-cycle	P2	TBD	TBD	TBD
		"	*c. Document changes to the location (i.e., system or system components) where the information is processed and stored.*	Zero-cycle	P2	TBD	TBD	TBD
	CM-12(1)	*(1) INFORMATION LOCATION | AUTOMATED TOOLS TO SUPPORT INFORMATION LOCATION*	*Use automated tools to identify CJI on software and hardware system components to ensure controls are in place to protect organizational information and individual privacy.*	Zero-cycle	P2	TBD	TBD	TBD

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy Section 5-8: Media Protection (MP)								
5.8: MP-1	5.8: MP-1	Policy and Procedures	a. Develop, document, and disseminate to authorized individuals:	Existing	P2	Agency	Agency	Agency
		"	1. Agency-level media protection policy that:	Existing	P2	Agency	Agency	Agency
		"	(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance; and	Existing	P2	Agency	Agency	Agency
		"	(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and	Existing	P2	Agency	Agency	Agency
		"	2. Procedures to facilitate the implementation of the media protection policy and the associated media protection controls;	Existing	P2	Agency	Agency	Agency
		"	b. Designate an individual with security responsibilities to manage the development, documentation, and dissemination of the media protection policy and procedures; and	Existing	P2	Agency	Agency	Agency
		"	c. Review and update the current media protection:	Zero-cycle	P2	Agency	Agency	Agency
		"	1. Policy at least annually and following any security incidents involving digital and/or non-digital media; and	Zero-cycle	P2	Agency	Agency	Agency
		"	2. Procedures at least annually and following any security incidents involving digital and/or non-digital media.	Zero-cycle	P2	Agency	Agency	Agency
5.8: MP-2	5.8: MP-2	Media Access	Restrict access to digital and non-digital media to authorized individuals.	Existing	P2	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	Zero-cycle	P3	Both	Both	Both
		"	b. Exempt digital and non-digital media containing CJI from marking if the media remain within physically secure locations and controlled areas.	Zero-cycle	P3	Both	Both	Both
5.8: MP-4	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	Existing	P2	Both	Both	Both
		"	b. Protect system media types defined in MP-4a until the media are destroyed or sanitized using approved equipment, techniques, and procedures.	Existing	P2	Both	Both	Both
5.8: MP-5	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 Section 5.10.1.2 of this Policy. Physical media will be protected at the same level as the information would be protected in electronic form. Restrict the activities associated with transport of electronic and physical media to authorized personnel;	Existing	P2	Agency	Both	Both
		"	b. Maintain accountability for system media during transport outside of the physically secure location or controlled areas;	Existing	P2	Both	Both	Both
		"	c. Document activities associated with the transport of system media; and	Existing	P2	Both	Both	Both
		"	d. Restrict the activities associated with the transport of system media to authorized personnel.	Existing	P2	Both	Both	Both
5.8: MP-6	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	Existing	P2	Agency	Both	Both

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	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.	Existing	P2	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	Existing	P2	Agency	Both	Both
		"	b. Prohibit the use of personally-owned digital media devices on all agency-owned or controlled systems that store, process, or transmit criminal justice information; and	Existing	P2	Agency	Both	Both
		"	c. Prohibit the use of digital media devices on all agency-owned or controlled systems that store, process, or transmit criminal justice information when such devices have no identifiable owner.	Existing	P2	Agency	Both	Both

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy Section 5-9: Physical Protection								
PE-1	PE-1	POLICY AND PROCEDURES	a. Develop, document, and disseminate to organizational personnel with physical and environmental protection responsibilities:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. Agency-level physical and environmental protection policy that:	Zero-cycle	P2	TBD	TBD	TBD
		"	(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Zero-cycle	P2	TBD	TBD	TBD
		"	(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and	Zero-cycle	P2	TBD	TBD	TBD
		"	2. Procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental protection controls;	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Designate organizational personnel with information security responsibilities to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures; and	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Review and update the current physical and environmental protection:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. Policy annually and following any physical, environmental, or security related incidents involving CJI or systems used to process, store, or transmit CJI; and	Zero-cycle	P2	TBD	TBD	TBD
		"	2. Procedures annually and following any physical, environmental, or security related incidents involving CJI or systems used to process, store, or transmit CJI.	Zero-cycle	P2	TBD	TBD	TBD
PE-2	PE-2	PHYSICAL ACCESS AUTHORIZATIONS	a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides;	Existing	P2	Both	Both	Both
		"	b. Issue authorization credentials for facility access;	Existing	P2	Both	Both	Both
		"	c. Review the access list detailing authorized facility access by individuals annually and when personnel changes occur; and	Existing	P2	Both	Both	Both
		"	d. Remove individuals from the facility access list when access is no longer required.	Existing	P2	Both	Both	Both
PE-3	PE-3	PHYSICAL ACCESS CONTROL	a. Enforce physical access authorizations by:	Existing	P2	Both	Both	Both
		"	1. Verifying individual access authorizations before granting access to the facility; and	Existing	P2	Both	Both	Both
		"	2. Controlling ingress and egress to the facility using agency-implemented procedures and controls;	Existing	P2	Both	Both	Both
		"	b. Maintain physical access audit logs for the physically secure location and agency-defined sensitive areas;	Existing	P2	Both	Both	Both
		"	c. Control access to areas within the facility designated as non-publicly accessible by implementing physical access devices including, but not limited to keys, locks, combinations, biometric readers, placards, and/or card readers;	Existing	P2	Both	Both	Both
		"	d. Escort visitors and control visitor activity in all physically secure locations;	Existing	P2	Both	Both	Both
		"	e. Secure keys, combinations, and other physical access devices;	Existing	P2	Both	Both	Both
		"	f. Inventory all agency-issued physical access devices annually; and	Existing	P2	Both	Both	Both
		"	g. Change combinations and keys ~~and/or~~ when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated.	Existing	P2	Both	Both	Both
		"	h. If the above conditions cannot be met refer to the requirements listed in PE-17.	Existing	P2	Both	Both	Both
PE-4	PE-4	ACCESS CONTROL FOR TRANSMISSION	Control physical access to information system distribution and transmission lines and devices within organizational facilities using agency-implemented procedures and controls.	Existing	P2	Both	Both	Both
PE-5	PE-5	ACCESS CONTROL FOR OUTPUT DEVICES	Control physical access to output from monitors, printers, scanners, audio devices, facsimile machines, and copiers to prevent unauthorized individuals from obtaining the output.	Existing	P3	Both	Both	Both

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
PE-6	PE-6	MONITORING PHYSICAL ACCESS	a. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents;	Existing	P2	Both	Both	Both
		"	b. Review physical access logs quarterly and upon occurrence of any physical, environmental, or security-related incidents involving CJI or systems used to process, store, or transmit CJI; and	Existing	P2	Both	Both	Both
		"	c. Coordinate results of reviews and investigations with the organizational incident response capability.	Existing	P2	Both	Both	Both
PE-6 (1)	PE-6 (1)	(1) MONITORING PHYSICAL ACCESS | INTRUSION ALARMS AND SURVEILLANCE EQUIPMENT	Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment.	Existing	P2	Both	Both	Both
PE-8	PE-8	VISITOR ACCESS RECORDS	a. Maintain visitor access records to the facility where the system resides for one (1) year;	Zero-cycle	P4	TBD	TBD	TBD
		"	b. Review visitor access records quarterly; and	Zero-cycle	P4	TBD	TBD	TBD
		"	c. Report anomalies in visitor access records to organizational personnel with physical and environmental protection responsibilities and organizational personnel with information security responsibilities.	Zero-cycle	P4	TBD	TBD	TBD
PE-8 (3)	PE-8 (3)	(3) VISITOR ACCESS RECORDS | LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS	Limit personally identifiable information contained in visitor access records to the minimum PII necessary to achieve the purpose for which it is collected (see Section 4.3).	Zero-cycle	P4	TBD	TBD	TBD
		"	Note: Access to visitor access records is restricted to authorized agency personnel.	Zero-cycle	P4	TBD	TBD	TBD
PE-9	PE-9	POWER EQUIPMENT AND CABLING	Protect power equipment and power cabling for the system from damage and destruction.	Zero-cycle	P2	TBD	TBD	TBD
PE-10	PE-10	EMERGENCY SHUTOFF	a. Provide the capability of shutting off power to all information systems in emergency situations;	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Place emergency shutoff switches or devices in easily accessible locations to facilitate access for authorized personnel; and	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Protect emergency power shutoff capability from unauthorized activation.	Zero-cycle	P2	TBD	TBD	TBD
PE-11	PE-11	EMERGENCY POWER	Provide an uninterruptible power supply to facilitate an orderly shutdown of the information system or transition of the information system to an alternate power source in the event of a primary power source loss.	Zero-cycle	P2	TBD	TBD	TBD
PE-12	PE-12	EMERGENCY LIGHTING	Employ and maintain automatic emergency lighting for the system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.	Zero-cycle	P2	TBD	TBD	TBD
PE-13	PE-13	FIRE PROTECTION	Employ and maintain fire detection and suppression systems that are supported by an independent energy source.	Zero-cycle	P2	TBD	TBD	TBD
PE-13 (1)	PE-13 (1)	(1) FIRE PROTECTION | DETECTION SYSTEMS — AUTOMATIC ACTIVATION AND NOTIFICATION	Employ fire detection systems that activate automatically and notify organizational personnel with physical and environmental protection responsibilities and police, fire, or emergency medical personnel in the event of a fire.	Zero-cycle	P2	TBD	TBD	TBD
PE-14	PE-14	ENVIRONMENTAL CONTROLS	a. Maintain adequate HVAC levels within the facility where the system resides at recommended system manufacturer levels; and	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Monitor environmental control levels continuously.	Zero-cycle	P2	TBD	TBD	TBD
PE-15	PE-15	WATER DAMAGE PROTECTION	Protect the system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.	Zero-cycle	P2	TBD	TBD	TBD
PE-16	PE-16	DELIVERY AND REMOVAL	a. Authorize and control information system-related components entering and exiting the facility; and	Existing	P3	Both	Both	Both
		"	b. Maintain records of the system components.	Existing	P3	Both	Both	Both

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
PE-17	PE-17	ALTERNATE WORK SITE	a. Determine and document all alternate facilities or locations allowed for use by employees;	Existing	P3	Both	Both	Both
		"	b. Employ the following controls at alternate work sites:	Existing	P3	Both	Both	Both
		"	1. Limit access to the area during CJI processing times to only those personnel authorized by the agency to access or view CJI.	Existing	P3	Both	Both	Both
		"	2. Lock the area, room, or storage container when unattended.	Existing	P3	Both	Both	Both
		"	3. Position information system devices and documents containing CJI in such a way as to prevent unauthorized individuals from access and view.	Existing	P3	Both	Both	Both
		"	4. Follow the encryption requirements found in SC-13 and SC-28 for electronic storage (i.e., data at-rest) of CJI.	Existing	P3	Both	Both	Both
		"	c. Assess the effectiveness of controls at alternate work sites; and	Existing	P3	Both	Both	Both
		"	d. Provide a means for employees to communicate with information security and privacy personnel in case of incidents.	Existing	P3	Both	Both	Both

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy Section 5-10: Systems and Communications Protection								
SC-1	SC-1	POLICY AND PROCEDURES	a. Develop, document, and disseminate to organizational personnel with system and communications protection responsibilities:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. Agency-level system and communications protection policy that:	Zero-cycle	P2	TBD	TBD	TBD
		"	(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Zero-cycle	P2	TBD	TBD	TBD
		"	(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and	Zero-cycle	P2	TBD	TBD	TBD
		"	2. Procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls;	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Designate organizational personnel with information security responsibilities to manage the development, documentation, and dissemination of the system and communications protection policy and procedures; and	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Review and update the current system and communications protection:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. Policy annually and following any changes and security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI; and	Zero-cycle	P2	TBD	TBD	TBD
		"	2. Procedures annually and following any changes and security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.	Zero-cycle	P2	TBD	TBD	TBD
SC-2	SC-2	SEPARATION OF SYSTEM AND USER FUNCTIONALITY	Separate user functionality, including user interface services, from system management functionality.	Existing	P2	Both	Service Provider	Service Provider
SC-4	SC-4	INFORMATION IN SHARED SYSTEM RESOURCES	Prevent unauthorized and unintended information transfer via shared system resources.	Existing	P2	TBD	TBD	TBD
SC-5	SC-5	DENIAL-OF-SERVICE PROTECTION	a. Protect against or limit the effects of the following types of denial-of-service events: distributed denial of service, DNS Denial of Service, etc.; and	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Employ the following controls to achieve the denial-of-service objective: boundary protection devices and intrusion detection or prevention devices.	Zero-cycle	P2	TBD	TBD	TBD
SC-7	SC-7	BOUNDARY PROTECTION	a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system;	Existing	P1	Both	Service Provider	Service Provider
		"	b. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal organizational networks; and	Existing	P1	Both	Service Provider	Service Provider
		"	c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.	Existing	P1	Both	Service Provider	Service Provider
SC-7 (3)	SC-7 (3)	BOUNDARY PROTECTION | ACCESS POINTS	Limit the number of external network connections to the system.	10/1/2024	P1	TBD	TBD	TBD
SC-7 (4)	SC-7 (4)	BOUNDARY PROTECTION | EXTERNAL TELECOMMUNICATIONS SERVICES	(a) Implement a managed interface for each external telecommunication service;	10/1/2024	P1	TBD	TBD	TBD
		"	(b) Establish a traffic flow policy for each managed interface;	10/1/2024	P1	TBD	TBD	TBD
		"	(c) Protect the confidentiality and integrity of the information being transmitted across each interface;	10/1/2024	P1	TBD	TBD	TBD
		"	(d) Document each exception to the traffic flow policy with a supporting mission or business need and duration of that need;	10/1/2024	P1	TBD	TBD	TBD

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
SC-7 (4)	SC-7 (4)	BOUNDARY PROTECTION | EXTERNAL TELECOMMUNICATIONS SERVICES (continued)	(e) Review exceptions to the traffic flow policy annually, after any incident, and after any major changes impacting the information system, while remove exceptions that are no longer supported by an explicit mission or business need;	10/1/2024	P1	TBD	TBD	TBD
		"	(f) Prevent unauthorized exchange of control plane traffic with external networks;	10/1/2024	P1	TBD	TBD	TBD
		"	(g) Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks; and	10/1/2024	P1	TBD	TBD	TBD
		"	(h) Filter unauthorized control plane traffic from external networks.	10/1/2024	P1	TBD	TBD	TBD
SC-7 (5)	SC-7 (5)	BOUNDARY PROTECTION | DENY BY DEFAULT — ALLOW BY EXCEPTION	Deny network communications traffic by default and allow network communications traffic by exception at boundary devices for information systems used to process, store, or transmit CJI.	10/1/2024	P1	TBD	TBD	TBD
SC-7 (7)	SC-7 (7)	BOUNDARY PROTECTION | SPLIT TUNNELING FOR REMOTE DEVICES	Prevent split tunneling for remote devices connecting to organizational systems.	10/1/2024	P1	TBD	TBD	TBD
SC-7 (8)	SC-7 (8)	BOUNDARY PROTECTION | ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS	Route all internal communications traffic that may be proxied, except traffic specifically exempted by organizational personnel with information security responsibilities, to all untrusted networks through authenticated proxy servers at managed interfaces.	Existing	P1	Both	Service Provider	Service Provider
SC-7 (24)	SC-7 (24)	BOUNDARY PROTECTION | PERSONALLY IDENTIFIABLE INFORMATION	For systems that process personally identifiable information:	10/1/2024	P1	TBD	TBD	TBD
		"	(a) Apply the following processing rules to data elements of personally identifiable information: all applicable laws, executive orders, directives, regulations, policies, standards, and guidelines;	10/1/2024	P1	TBD	TBD	TBD
		"	(b) Monitor for permitted processing at the external interfaces to the system and at key internal boundaries within the system;	10/1/2024	P1	TBD	TBD	TBD
		"	(c) Document each processing exception; and	10/1/2024	P1	TBD	TBD	TBD
		"	(d) Review and remove exceptions that are no longer supported.	10/1/2024	P1	TBD	TBD	TBD
SC-8	SC-8	TRANSMISSION CONFIDENTIALITY AND INTEGRITY	Protect the confidentiality and integrity of transmitted information.	Existing	P2	Both	Service Provider	Service Provider
		"	Metadata derived from unencrypted CJI shall be protected in the same manner as CJI and shall not be used for any advertising or other commercial purposes by any cloud service provider or other associated entity.	Existing	P2	Service Provider	Service Provider	Service Provider
SC-8 (1)	SC-8 (1)	TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC PROTECTION	Implement cryptographic mechanisms to prevent unauthorized disclosure and detect unauthorized changes or access to CJI during transmission.	Existing	P2	Both	Service Provider	Service Provider
SC-10	SC-10	NETWORK DISCONNECT	Terminate the network connection associated with a communications session at the end of the session or after one (1) hour of inactivity.	Zero-cycle	P3	TBD	TBD	TBD
		"	NOTE: In the interest of safety, devices that are: (1) part of a criminal justice conveyance; or (2) used to perform dispatch functions and located within a physically secure location; or (3) terminals designated solely for the purpose of receiving alert notifications (i.e., receive only terminals or ROT) and used within physically secure location facilities that remain staffed when in operation, are exempt from this requirement.	Zero-cycle	P3	TBD	TBD	TBD

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
SC-12	SC-12	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: encryption key generation, distribution, storage, access, and destruction is controlled by the agency.	Existing	P2	TBD	TBD	TBD
SC-13	SC-13	CRYPTOGRAPHIC PROTECTION	a. Determine the use of encryption for CJI in-transit when outside a physically secure location; and	Existing	P2	TBD	TBD	TBD
		"	b. Implement the following types of cryptography required for each specified cryptographic use: cryptographic modules which are Federal Information Processing Standard (FIPS) 140-3 certified, or FIPS validated algorithm for symmetric key encryption and decryption (FIPS 197 [AES]), with a symmetric cipher key of at least 128-bit strength for CJI in-transit.	Existing	P2	TBD	TBD	TBD
		"	NOTE: Subsequent versions of approved cryptographic modules that are under current review for FIPS 140-3 compliancy can be used in the interim until certification is complete. FIPS 140-2 certificates will not be acceptable after September 21, 2026.	Existing	P2	TBD	TBD	TBD
SC-15	SC-15	COLLABORATIVE COMPUTING DEVICES AND APPLICATIONS	a. Prohibit remote activation of collaborative computing devices and applications; and	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Provide an explicit indication of use to users physically present at the devices.	Zero-cycle	P2	TBD	TBD	TBD
SC-17	SC-17	PUBLIC KEY INFRASTRUCTURE CERTIFICATES	a. Issue public key certificates under an agency-level certificate authority or obtain public key certificates from an approved service provider; and	Existing	P2	Both	Service Provider	Service Provider
		"	b. Include only approved trust anchors in trust stores or certificate stores managed by the organization.	Existing	P2	Both	Service Provider	Service Provider
SC-18	SC-18	MOBILE CODE	a. Define acceptable and unacceptable mobile code and mobile code technologies; and	Zero-cycle	P3	TBD	TBD	TBD
		"	b. Authorize, monitor, and control the use of mobile code within the system.	Zero-cycle	P3	TBD	TBD	TBD
SC-20	SC-20	SECURE NAME/ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)	a. Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.	Zero-cycle	P2	TBD	TBD	TBD
SC-21	SC-21	SECURE NAME/ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)	Request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.	Zero-cycle	P2	TBD	TBD	TBD
SC-22	SC-22	ARCHITECTURE AND PROVISIONING FOR NAME/ADDRESS RESOLUTION SERVICE	Ensure the systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal and external role separation.	Zero-cycle	P2	TBD	TBD	TBD
SC-23	SC-23	SESSION AUTHENTICITY	Protect the authenticity of communications sessions.	Zero-cycle	P2	TBD	TBD	TBD

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
SC-28	SC-28	PROTECTION OF INFORMATION AT REST	Protect the confidentiality and integrity of the following information at rest: CJI when outside physically secure locations using cryptographic modules which are certified FIPS 140-3 with a symmetric cipher key of at least 128-bit strength, or FIPS 197 with a symmetric cipher key of at least 256-bit strength.	Existing	P2	Both	Service Provider	Service Provider
		"	Metadata derived from unencrypted CJI shall be protected in the same manner as CJI and shall not be used for any advertising or other commercial purposes by any cloud service provider or other associated entity.	Existing	P2	Both	Service Provider	Service Provider
		"	The storage of CJI, regardless of encryption status, shall only be permitted in cloud environments (e.g., government or third-party/commercial datacenters, etc.) which reside within the physical boundaries of APB-member country (i.e., United States, U.S. territories, Indian Tribes, and Canada) and are under legal authority of an APB-member agency (i.e., United States–federal/state/territory, Indian Tribe, or the Royal Canadian Mounted Police).	Existing	P2	Both	Service Provider	Service Provider
		"	Note: This restriction does not apply to exchanges of CJI with foreign government agencies under international exchange agreements (e.g., the Preventing and Combating Serious Crime agreements, fugitive extracts, and exchanges made for humanitarian and criminal investigatory purposes in particular circumstances).	Existing	P2	Both	Service Provider	Service Provider
SC-28 (1)	SC-28 (1)	PROTECTION OF INFORMATION AT REST | CRYPTOGRAPHIC PROTECTION	Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on information systems and digital media outside physically secure locations: CJI.	Existing	P2	Both	Service Provider	Service Provider
SC-39	SC-39	PROCESS ISOLATION	Maintain a separate execution domain for each executing system process.	Existing	P2	Both	Service Provider	Service Provider

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy Section 5-11: 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.	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
		"	This audit **shall** include a sample of CJAs and, in coordination with the SIB, the NCJAs.	Existing	Existing	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.	Existing	Existing	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.	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
5.11.2	5.11.2	Audits by the CSA	Each CSA **shall**:	Existing	Existing			
		"	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.	Existing	Existing	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.	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
		"	3. Have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.	Existing	Existing	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.	Existing	Existing	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.	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
		"	The inspection team **shall** be appointed by the APB and…	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
		"	...and **shall** include at least one representative of the CJIS Division.	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO
		"	All results of the inquiry and audit **shall** be reported to the APB with appropriate recommendations.	Existing	Existing	CJIS/CSO	CJIS/CSO	CJIS/CSO

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy Section 5-12: 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).	Existing	Existing	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.	Existing	Existing	Agency	Agency	Agency
		"	When appropriate, the screening **shall** be consistent with:	Existing	Existing	Agency	Agency	Agency
		"	a. 5 CFR 731.106; and/or	Existing	Existing	Agency	Agency	Agency
		"	b. Office of Personnel Management policy, regulations, and guidance; and/or	Existing	Existing	Agency	Agency	Agency
		"	c. agency policy, regulations, and guidance.	Existing	Existing	Agency	Agency	Agency
		"	2. All requests for access **shall** be made as specified by the CSO.	Existing	Existing	Agency	Agency	Agency
		"	All CSO designees **shall** be from an authorized criminal justice agency.	Existing	Existing	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.	Existing	Existing	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.	Existing	Existing	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.	Existing	Existing	Agency	Agency	Agency
		"	c. (cont) The CGA **shall** in turn notify the contractor's security officer.	Existing	Existing	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.	Existing	Existing	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.	Existing	Existing	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…	Existing	Existing	Agency	Agency	Agency
		"	...and the person's appointing authority **shall** be notified in writing of the access denial.	Existing	Existing	Agency	Agency	Agency
		"	7. The granting agency **shall** maintain a list of personnel who have been authorized unescorted access to unencrypted CJI and...	Existing	Existing	Agency	Agency	Agency
		"	...and **shall**, upon request, provide a current copy of the access list to the CSO.	Existing	Existing	Agency	Agency	Agency
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.	Existing	Existing	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.	Existing	Existing	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.	Existing	Existing	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.	Existing	Existing	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.	Existing	Existing	Both	Both	Both

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy Section 5-13: Mobile Devices								
5.13	5.13	Mobile Devices	The agency **shall**:	Existing	Existing			
		"	(i) establish usage restrictions and implementation guidance for mobile devices;	Existing	Existing	Agency	Agency	Agency
		"	(ii) authorize, monitor, control wireless access to the information system.	Existing	Existing	Agency	Agency	Agency
5.13.1.1	5.13.1.1	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.	Existing	Existing	Agency	Agency	Agency
		"	Agencies **shall** implement the following controls for all agency-managed wireless access points with access to an agency's network that processes unencrypted CJI:	Existing	Existing	Agency	Agency	Agency
		"	1. Perform validation testing to ensure rogue APs (Access Points) do not exist in the 802.11 Wireless Local Area Network (WLAN) and to fully understand the wireless network security posture.	Existing	Existing	Agency	Agency	Agency
		"	2. Maintain a complete inventory of all Access Points (APs) and 802.11 wireless devices.	Existing	Existing	Agency	Agency	Agency
		"	3. Place APs in secured areas to prevent unauthorized physical access and user manipulation.	Existing	Existing	Agency	Agency	Agency
		"	4. Test AP range boundaries to determine the precise extent of the wireless coverage and design the AP wireless coverage to limit the coverage area to only what is needed for operational purposes.	Existing	Existing	Agency	Agency	Agency
		"	5. Enable user authentication and encryption mechanisms for the management interface of the AP.	Existing	Existing	Agency	Agency	Agency
		"	6. Ensure that all APs have strong administrative passwords and ensure that all passwords are changed in accordance with section 5.6.3.1.	Existing	Existing	Agency	Agency	Agency
		"	7. Ensure the reset function on APs is used only when needed and is only invoked by authorized personnel. Restore the APs to the latest security settings, when the reset functions are used, to ensure the factory default settings are not utilized.	Existing	Existing	Agency	Agency	Agency
		"	8. Change the default service set identifier (SSID) in the APs.	Existing	Existing	Agency	Agency	Agency
		"	Disable the broadcast SSID feature so that the client SSID must match that of the AP.	Existing	Existing	Agency	Agency	Agency
		"	Validate that the SSID character string does not contain any agency identifiable information (division, department, street, etc.) or services.	Existing	Existing	Agency	Agency	Agency
		"	9. Enable all security features of the wireless product, including the cryptographic authentication, firewall, and other privacy features.	Existing	Existing	Agency	Agency	Agency
		"	10. Ensure that encryption key sizes are at least 128-bits and…	Existing	Existing	Agency	Agency	Agency
		"	...and the default shared keys are replaced by unique keys.	Existing	Existing	Agency	Agency	Agency
		"	11. Ensure that the ad hoc mode has been disabled.	Existing	Existing	Agency	Agency	Agency
		"	12. Disable all nonessential management protocols on the APs. Disable non-FIPS compliant secure access to the managment interface.	Existing	Existing	Agency	Agency	Agency
		"	13. Ensure all management access and authentication occurs via FIPS compliant secure protocols (e.g. SFTP, HTTPS, SNMP over TLS, etc.). Disable non-FIPS compliant secure access to the managment interface.	Existing	Existing	Agency	Agency	Agency
		"	14. Enable logging (if supported) and…	Existing	Existing	Agency	Agency	Agency
		"	...and review the logs on a recurring basis per local policy.	Existing	Existing	Agency	Agency	Agency
		"	At a minimum logs **shall** be reviewed monthly.	Existing	Existing	Agency	Agency	Agency

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
5.13.1.1	5.13.1.1	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.	Existing	Existing	Agency	Agency	Agency
		"	16. When disposing of access points that will no longer be used by the agency, clear access point configuration to prevent disclosure of network configuration, keys, passwords, etc.	Existing	Existing	Agency	Agency	Agency
5.13.1.2.1	5.13.1.2.1	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.	Existing	Existing	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.	Existing	Existing	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:	Existing	Existing			
		"	1. Enable encryption on the hotspot	Existing	Existing	Agency	Agency	Agency
		"	2. Change the hotspot's default SSID	Existing	Existing	Agency	Agency	Agency
		"	a. Ensure the hotspot SSID does not identify the device make/model or agency ownership	Existing	Existing	Agency	Agency	Agency
		"	3. Create a wireless network password (Pre-shared key)	Existing	Existing	Agency	Agency	Agency
		"	4. Enable the hotspot's port filtering/blocking features if present	Existing	Existing	Agency	Agency	Agency
		"	5. Only allow connections from agency controlled devices	Existing	Existing	Agency	Agency	Agency
		"	OR 1. Have a MDM solution to provide the same security as identified in 1 - 5 above.	Existing	Existing	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.	Existing	Existing	Agency	Agency	Agency
		"	User agencies **shall** implement the following controls when directly accessing CJI from devices running limited feature operating system:	Existing	Existing			
		"	1. Ensure that CJI is only transferred between CJI authorized applications and storage areas of the device.	Existing	Existing	Agency	Agency	Agency
		"	2. MDM with centralized administration configured and implemented to perform at least the following controls:	Existing	Existing	Agency	Agency	Agency
		"	a. Remote locking of the device	Existing	Existing	Agency	Agency	Agency
		"	b. Remote wiping of the device	Existing	Existing	Agency	Agency	Agency
		"	c. Setting and locking device configuration	Existing	Existing	Agency	Agency	Agency
		"	d. Detection of "rooted" and "jailbroken" devices	Existing	Existing	Agency	Agency	Agency
		"	e. Enforcement of folder or disk level encryption	Existing	Existing	Agency	Agency	Agency
		"	f. Application of mandatory policy settings on the device	Existing	Existing	Agency	Agency	Agency
		"	g. Detection of unauthorized configurations	Existing	Existing	Agency	Agency	Agency
		"	h. Detection of unauthorized software or applications	Existing	Existing	Agency	Agency	Agency
		"	i. Ability to determine location of agency controlled devices	Existing	Existing	Agency	Agency	Agency
		"	j. Prevention of unpatched devices from accessing CJI or CJI systems	Existing	Existing	Agency	Agency	Agency
		"	k. Automatic device wiping after a specified number of failed access attempts	Existing	Existing	Agency	Agency	Agency

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	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:	Existing	Existing			
		"	1. Apply available critical patches and upgrades to the operating system as soon as they become available for the device and after necessary testing as described in Section 5.10.4.1.	Existing	Existing	Agency	Agency	Agency
		"	2. Are configured for local device authentication (see Section 5.13.8.1).	Existing	Existing	Agency	Agency	Agency
		"	3. Use advanced authentication or CSO approved compensating controls as per Section 5.13.7.2.1.	Existing	Existing	Agency	Agency	Agency
		"	4. Encrypt all CJI resident on the device.	Existing	Existing	Agency	Agency	Agency
		"	5. Erase cached information, to include authenticators (see Section 5.6.2.1) in applications, when session is terminated.	Existing	Existing	Agency	Agency	Agency
		"	6. Employ personal firewalls on full-featured operating system devices or run a Mobile Device Management (MDM) system that facilitates the ability to provide firewall services from the agency level.	Existing	Existing	Agency	Agency	Agency
		"	7. Employ malicious code protection on full-featured operating system devices or run a MDM system that facilitates the ability to provide anti-malware services from the agency level.	Existing	Existing	Agency	Agency	Agency
5.13.4.1	5.13.4.1	Patching/Updates	Agencies **shall** monitor mobile devices to ensure their patch and update state is current.	Existing	Existing	Agency	Agency	Agency
5.13.4.2	5.13.4.2	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.	Existing	Existing	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).	Existing	Existing	Agency	Agency	Agency
		"	At a minimum, the personal firewall **shall** perform the following activities:	Existing	Existing			
		"	1. Manage program access to the Internet.	Existing	Existing	Agency	Agency	Agency
		"	2. Block unsolicited requests to connect to the PC.	Existing	Existing	Agency	Agency	Agency
		"	3. Filter Incoming traffic by IP address or protocol.	Existing	Existing	Agency	Agency	Agency
		"	4. Filter Incoming traffic by destination ports.	Existing	Existing	Agency	Agency	Agency
		"	5. Maintain an IP traffic log.	Existing	Existing	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.	Existing	Existing	Agency	Agency	Agency
		"	Special reporting procedures for mobile devices **shall** apply in any of the following situations:	Existing	Existing			
		"	1. Loss of device control. For example:	Existing	Existing	Agency	Agency	Agency
		"	a. Device known to be locked, minimal duration of loss	Existing	Existing	Agency	Agency	Agency
		"	b. Device lock state unknown, minimal duration of loss	Existing	Existing	Agency	Agency	Agency
		"	c. Device lock state unknown, extended duration of loss	Existing	Existing	Agency	Agency	Agency
		"	d. Device known to be unlocked, more than momentary duration of loss	Existing	Existing	Agency	Agency	Agency
		"	2. Total loss of device	Existing	Existing	Agency	Agency	Agency
		"	3. Device compromise	Existing	Existing	Agency	Agency	Agency
		"	4. Device loss or compromise outside the United States	Existing	Existing	Agency	Agency	Agency
5.13.6	5.13.6	Access Control	Access control (Section 5.5 Access Control) **shall** be accomplished by the application that accesses CJI.	Existing	Existing	Agency	Agency	Agency
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.	Existing	Existing	Agency	Agency	Agency
		"	The authenticator used **shall** meet the requirements in section 5.6.2.1 Standard Authenticators.	Existing	Existing	Agency	Agency	Agency

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
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 in indirect, then AA is not required.	Existing	Existing	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.	Existing	Existing	Agency	Agency	Agency
		"	The compensating controls **shall:**	Existing	Existing			
		"	1. Meet the intent of the CJIS Security Policy AA requirement	Existing	Existing	Agency	Agency	Agency
		"	2. Provide a similar level of protection or security as the original AA requirement	Existing	Existing	Agency	Agency	Agency
		"	3. Not rely upon the existing requirements for AA as compensating controls	Existing	Existing	Agency	Agency	Agency
		"	4. Expire upon the CSO approved date or when a compliant AA solution is implemented.	Existing	Existing	Agency	Agency	Agency
		"	The following minimum controls **shall** be implemented as a part of the CSO approved compensating controls:	Existing	Existing			
		"	Possession and registration of an agency-issued smartphone or tablet as an indication it is the authorized user	Existing	Existing	Agency	Agency	Agency
		"	Use of device certificates as per Section 5.13.7.3 Device Certificates	Existing	Existing	Agency	Agency	Agency
		"	Implemented CJIS Security Policy compliant standard authenticator protection on the secure location where CJI is stored	Existing	Existing	Agency	Agency	Agency
5.13.7.3	5.13.7.3	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:	Existing	Existing			
		"	1. Protected against being extracted from the device	Existing	Existing	Agency	Agency	Agency
		"	2. Configured for remote wipe on demand or self-deletion based on a number of unsuccessful login or access attempts	Existing	Existing	Agency	Agency	Agency
		"	3. Configured to use a secure authenticator (i.e. password, PIN) to unlock the key for use	Existing	Existing	Agency	Agency	Agency

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy Section 5-14: 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	Zero-cycle	P2	Both	Both	Both
		"	b. Provide the following option for alternative sources for continued support for unsupported components: original manufacturer support, or original contracted vendor support.	Zero-cycle	P2	Both	Both	Both

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy Section 5-15: 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:	Zero-cycle	P2	Agency	Agency	Agency
		"	1. Agency-level system and information integrity policy that:	Zero-cycle	P2	Agency	Agency	Agency
		"	(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Zero-cycle	P2	Agency	Agency	Agency
		"	(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and	Zero-cycle	P2	Agency	Agency	Agency
		"	2. Procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls;	Zero-cycle	P2	Agency	Agency	Agency
		"	b. Designate organizational personnel with system and information integrity responsibilities to manage the development, documentation, and dissemination of the system and information integrity policy and procedures; and	Zero-cycle	P2	Agency	Agency	Agency
		"	c. Review and update the current system and information integrity:	Zero-cycle	P2	Agency	Agency	Agency
		"	1. Policy annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI; and	Zero-cycle	P2	Agency	Agency	Agency
		"	2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.	Zero-cycle	P2	Agency	Agency	Agency
5.15: SI-2	5.15: SI-2	FLAW REMEDIATION	a. Identify, report, and correct system flaws;	Existing	P1	Both	Service Provider	Service Provider
		"	b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;	10/1/2024	P1	Both	Service Provider	Service Provider
		"	c. Install security-relevant software and firmware updates within the number of days listed after the release of the updates;	Existing	P1	Both	Service Provider	Service Provider
		"	• Critical – 15 days	10/1/2024	P1	Both	Service Provider	Service Provider
		"	• High – 30 days	10/1/2024	P1	Both	Service Provider	Service Provider
		"	• Medium – 60 days	10/1/2024	P1	Both	Service Provider	Service Provider
		"	• Low – 90 days; and	10/1/2024	P1	Both	Service Provider	Service Provider
		"	d. Incorporate flaw remediation into the organizational configuration management process.	10/1/2024	P1	Both	Service Provider	Service Provider
5.15: SI-2 (2)	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.	10/1/2024	P1	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;	10/1/2024	P1	Both	Service Provider	Service Provider
		"	b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;	Existing	P1	Both	Service Provider	Service Provider
		"	c. Configure malicious code protection mechanisms to:	Existing	P1			
		"	1. Perform periodic scans of the system at least daily and real-time scans of files from external sources at network entry and exit points and on all servers and endpoint devices as the files are downloaded, opened, or executed in accordance with organizational policy; and	Existing	P1	Both	Service Provider	Service Provider

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
5.15: SI-3	5.15: SI-3	MALICIOUS CODE PROTECTION (continued)	2. Block or quarantine malicious code, take mitigating action(s), and when necessary, implement incident response procedures; and send alert to system/network administrators and/or organizational personnel with information security responsibilities in response to malicious code detection; and	10/1/2024	P1	Both	Service Provider	Service Provider
		"	d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.	10/1/2024	P1	Both	Service Provider	Service Provider
5.15: SI-4	5.15: SI-4	SYSTEM MONITORING	a. Monitor the system to detect:	10/1/2024	P1	Both	Service Provider	Service Provider
		"	1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives:	10/1/2024	P1	Both	Service Provider	Service Provider
		"	a. Intrusion detection and prevention	10/1/2024	P1	Both	Service Provider	Service Provider
		"	b. Malicious code protection	10/1/2024	P1	Both	Service Provider	Service Provider
		"	c. Vulnerability scanning	10/1/2024	P1	Both	Service Provider	Service Provider
		"	d. Audit record monitoring	10/1/2024	P1	Both	Service Provider	Service Provider
		"	e. Network monitoring	10/1/2024	P1	Both	Service Provider	Service Provider
		"	f. Firewall monitoring;	10/1/2024	P1	Both	Service Provider	Service Provider
		"	2. Unauthorized local, network, and remote connections;	10/1/2024	P1	Both	Service Provider	Service Provider
		"	b. Identify unauthorized use of the system through the following techniques and methods: event logging (ref. 5.4 Audit and Accountability);	10/1/2024	P1	Both	Service Provider	Service Provider
		"	c. Invoke internal monitoring capabilities or deploy monitoring devices:	10/1/2024	P1	Both	Service Provider	Service Provider
		"	1. Strategically within the system to collect organization-determined essential information; and	10/1/2024	P1	Both	Service Provider	Service Provider
		"	2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;	10/1/2024	P1	Both	Service Provider	Service Provider
		"	d. Analyze detected events and anomalies;	10/1/2024	P1	Both	Service Provider	Service Provider
		"	e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;	10/1/2024	P1	Both	Service Provider	Service Provider
		"	f. Obtain legal opinion regarding system monitoring activities; and	10/1/2024	P1	Both	Service Provider	Service Provider
		"	g. Provide intrusion detection and prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring, and firewall monitoring software logs to organizational personnel with information security responsibilities weekly.	10/1/2024	P1	Both	Service Provider	Service Provider
5.15: SI-4 (2)	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.	Existing	P1	Both	Service Provider	Service Provider

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
5.15: SI-4 (4)	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;	Existing	P1	Both	Service Provider	Service Provider
		"	b. Monitor inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions such as: the presence of malicious code or unauthorized use of legitimate code or credentials within organizational systems or propagating among system components, signaling to external systems, and the unauthorized exporting of information.	Existing	P1	Both	Service Provider	Service Provider
5.15: SI-4 (5)	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.	Existing	P1	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;	Existing	P2	Both	Service Provider	Service Provider
		"	b. Generate internal security alerts, advisories, and directives as deemed necessary;	Existing	P2	Both	Service Provider	Service Provider
		"	c. Issue security alerts, advisories, and directives to: organizational personnel implementing, operating, maintaining, and using the system; and	Existing	P2	Both	Service Provider	Service Provider
		"	d. Implement security directives in accordance with established time frames, or notify the issuing organization of the degree of noncompliance.	Existing	P2	Both	Service Provider	Service Provider
5.15: SI-7	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	10/1/2024	P1	Both	Service Provider	Service Provider
		"	b. Take the following actions when unauthorized changes to the software, firmware, and information are detected: notify organizational personnel responsible for software, firmware, and/or information integrity and implement incident response procedures as appropriate.	10/1/2024	P1	Both	Service Provider	Service Provider
5.15: SI-7 (1)	5.15: SI-7 (1)	(1) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY CHECKS	Perform an integrity check of software, firmware, and information systems that contain or process CJI at agency-defined transitional states or security relevant events at least weekly or in an automated fashion.	10/1/2024	P1	Both	Service Provider	Service Provider
5.15: SI-7 (7)	5.15: SI-7 (7)	(7) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRATION OF DETECTION AND RESPONSE	Incorporate the detection of the following unauthorized changes into the organizational incident response capability: unauthorized changes to established configuration setting or the unauthorized elevation of system privileges.	10/1/2024	P1	Both	Service Provider	Service Provider
5.15: SI-8	5.15: SI-8	SPAM PROTECTION	a. Employ spam protection mechanisms at system entry points to detect and act on unsolicited messages; and	Existing	P3	Both	Service Provider	Service Provider
		"	b. Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.	Existing	P3	Both	Service Provider	Service Provider
5.15: SI-8 (2)	5.15: SI-8 (2)	(2) SPAM PROTECTION | AUTOMATIC UPDATES	Automatically update spam protection mechanisms at least daily.	Zero-cycle	P3	Both	Service Provider	Service Provider
5.15: SI-10	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.	10/1/2024	P1	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	Zero-cycle	P3	Both	Service Provider	Service Provider
		"	b. Reveal error messages only to organizational personnel with information security responsibilities.	Zero-cycle	P3	Both	Service Provider	Service Provider
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.	Existing	P3	Both	Service Provider	Service Provider

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
5.15: SI-12 (1)	5.15: SI-12 (1)	(1) INFORMATION MANAGEMENT AND RETENTION | LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS	Limit personally identifiable information being processed in the information life cycle to the minimum PII necessary to achieve the purpose for which it is collected (see Section 4.3).	Existing	P3	Both	Service Provider	Service Provider
5.15: SI-12 (2)	5.15: SI-12 (2)	(2) INFORMATION MANAGEMENT AND RETENTION | MINIMIZE PERSONALLY IDENTIFIABLE INFORMATION IN TESTING, TRAINING, AND RESEARCH	Use the following techniques to minimize the use of personally identifiable information for research, testing, or training: data obfuscation, randomization, anonymization, or use of synthetic data.	Zero-cycle	P3	Both	Service Provider	Service Provider
5.15: SI-12 (3)	5.15: SI-12 (3)	(3) INFORMATION MANAGEMENT AND RETENTION | INFORMATION DISPOSAL	Use the following techniques to dispose of, destroy, or erase information following the retention period: as defined in MP-6.	Existing	P3	Both	Service Provider	Service Provider
5.15: SI-16	5.15: SI-16	MEMORY PROTECTION	Implement the following controls to protect the system memory from unauthorized code execution: data execution prevention and address space layout randomization.	Zero-cycle	P2	Both	Service Provider	Service Provider

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy Section 5-16: Maintenance (MA)								
MA-1	MA-1	POLICY AND PROCEDURES	a. Develop, document, and disseminate to organizational personnel with system maintenance responsibilities:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. Agency-level maintenance policy that:	Zero-cycle	P2	TBD	TBD	TBD
		"	(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Zero-cycle	P2	TBD	TBD	TBD
		"	(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and	Zero-cycle	P2	TBD	TBD	TBD
		"	2. Procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls;	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Designate organizational personnel with information security and privacy responsibilities to manage the development, documentation, and dissemination of the maintenance policy and procedures; and	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Review and update the current maintenance:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. Policy annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI; and	Zero-cycle	P2	TBD	TBD	TBD
		"	2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.	Zero-cycle	P2	TBD	TBD	TBD
MA-2	MA-2	CONTROLLED MAINTENANCE	a. Schedule, document, and review records of maintenance, repair, and replacement on system components in accordance with manufacturer or vendor specifications and/or organizational requirements;	Zero-cycle	P3	TBD	TBD	TBD
		"	b. Approve and monitor all maintenance activities, whether performed on site or remotely and whether the system or system components are serviced on site or removed to another location;	Zero-cycle	P3	TBD	TBD	TBD
		"	c. Require that organizational personnel with information security and privacy responsibilities explicitly approve the removal of the system or system components from organizational facilities for off-site maintenance, repair, or replacement;	Zero-cycle	P3	TBD	TBD	TBD
		"	d. Sanitize equipment to remove information from associated media prior to removal from organizational facilities for off-site maintenance, repair, replacement, or destruction;	Zero-cycle	P3	TBD	TBD	TBD
		"	e. Check all potentially impacted controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions; and	Zero-cycle	P3	TBD	TBD	TBD
		"	f. Include the following information in organizational maintenance records:	Zero-cycle	P3	TBD	TBD	TBD
		"	1. Component name	Zero-cycle	P3	TBD	TBD	TBD
		"	2. Component serial number	Zero-cycle	P3	TBD	TBD	TBD
		"	3. Date/time of maintenance	Zero-cycle	P3	TBD	TBD	TBD
		"	4. Maintenance performed	Zero-cycle	P3	TBD	TBD	TBD
		"	5. Name(s) of entity performing maintenance including escort if required.	Zero-cycle	P3	TBD	TBD	TBD
MA-3	MA-3	MAINTENANCE TOOLS	a. Approve, control, and monitor the use of system maintenance tools; and	Zero-cycle	P4	TBD	TBD	TBD
		"	b. Review previously approved system maintenance tools prior to each use.	Zero-cycle	P4	TBD	TBD	TBD
MA-3(1)	MA-3(1)	(1) MAINTENANCE TOOLS | INSPECT TOOLS	Inspect the maintenance tools used by maintenance personnel for improper or unauthorized modifications.	Zero-cycle	P4	TBD	TBD	TBD
MA-3(2)	MA-3(2)	(2) MAINTENANCE TOOLS | INSPECT MEDIA	Check media containing diagnostic and test programs for malicious code before the media are used in the system.	Zero-cycle	P4	TBD	TBD	TBD

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
MA-3(3)	MA-3(3)	(3) MAINTENANCE TOOLS | PREVENT UNAUTHORIZED REMOVAL	Prevent the removal of maintenance equipment containing organizational information by:	Zero-cycle	P4	TBD	TBD	TBD
		"	(a) Verifying that there is no organizational information contained on the equipment;	Zero-cycle	P4	TBD	TBD	TBD
		"	(b) Sanitizing or destroying the equipment;	Zero-cycle	P4	TBD	TBD	TBD
		"	(c) Retaining the equipment within the facility; or	Zero-cycle	P4	TBD	TBD	TBD
		"	(d) Obtaining an exemption from organizational personnel with system maintenance responsibilities explicitly authorizing removal of the equipment from the facility.	Zero-cycle	P4	TBD	TBD	TBD
MA-4	MA-4	NONLOCAL MAINTENANCE	a. Approve and monitor nonlocal maintenance and diagnostic activities;	Zero-cycle	P3	TBD	TBD	TBD
		"	b. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system;	Zero-cycle	P3	TBD	TBD	TBD
		"	c. Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions;	Zero-cycle	P3	TBD	TBD	TBD
		"	d. Maintain records for nonlocal maintenance and diagnostic activities; and	Zero-cycle	P3	TBD	TBD	TBD
		"	e. Terminate session and network connections when nonlocal maintenance is completed.	Zero-cycle	P3	TBD	TBD	TBD
MA-5	MA-5	MAINTENANCE PERSONNEL	a. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel;	Zero-cycle	P3	TBD	TBD	TBD
		"	b. Verify that non-escorted personnel performing maintenance on the system possess the required access authorizations; and	Zero-cycle	P3	TBD	TBD	TBD
		"	c. Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.	Zero-cycle	P3	TBD	TBD	TBD
MA-6	MA-6	TIMELY MAINTENANCE	Obtain maintenance support and/or spare parts for critical system components that process, store, and transmit CJI within agency-defined recovery time and recovery point objectives of failure.	Zero-cycle	P3	TBD	TBD	TBD

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy Area 5-17 - Planning (PL)								
PL-1	PL-1	POLICY AND PROCEDURES	a. Develop, document, and disseminate to organizational personnel with planning responsibilities:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. Agency-level planning policy that:	Zero-cycle	P2	TBD	TBD	TBD
		"	(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Zero-cycle	P2	TBD	TBD	TBD
		"	(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and	Zero-cycle	P2	TBD	TBD	TBD
		"	2. Procedures to facilitate the implementation of the planning policy and the associated planning controls;	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Designate organizational personnel with information security and privacy responsibilities to manage the development, documentation, and dissemination of the planning policy and procedures; and	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Review and update the current planning:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. Policy annually and following; any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI and	Zero-cycle	P2	TBD	TBD	TBD
		"	2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.	Zero-cycle	P2	TBD	TBD	TBD
PL-2	PL-2	SYSTEM SECURITY AND PRIVACY PLANS	a. Develop security and privacy plans for the system that:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. Are consistent with the organization's enterprise architecture;	Zero-cycle	P2	TBD	TBD	TBD
		"	2. Explicitly define the constituent system components;	Zero-cycle	P2	TBD	TBD	TBD
		"	3. Describe the operational context of the system in terms of mission and business processes;	Zero-cycle	P2	TBD	TBD	TBD
		"	4. Identify the individuals that fulfill system roles and responsibilities;	Zero-cycle	P2	TBD	TBD	TBD
		"	5. Identify the information types processed, stored, and transmitted by the system;	Zero-cycle	P2	TBD	TBD	TBD
		"	6. Provide the security categorization of the system, including supporting rationale;	Zero-cycle	P2	TBD	TBD	TBD
		"	7. Describe any specific threats to the system that are of concern to the organization;	Zero-cycle	P2	TBD	TBD	TBD
		"	8. Provide the results of a privacy risk assessment for systems processing personally identifiable information;	Zero-cycle	P2	TBD	TBD	TBD
		"	9. Describe the operational environment for the system and any dependencies on or connections to other systems or system components;	Zero-cycle	P2	TBD	TBD	TBD
		"	10. Provide an overview of the security and privacy requirements for the system;	Zero-cycle	P2	TBD	TBD	TBD
		"	11. Identify any relevant control baselines or overlays, if applicable;	Zero-cycle	P2	TBD	TBD	TBD
		"	12. Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions;	Zero-cycle	P2	TBD	TBD	TBD
		"	13. Include risk determinations for security and privacy architecture and design decisions;	Zero-cycle	P2	TBD	TBD	TBD
		"	14. Include security- and privacy-related activities affecting the system that require planning and coordination with organizational personnel with system security and privacy planning and plan implementation responsibilities; system developers; organizational personnel with information security and privacy responsibilities; and	Zero-cycle	P2	TBD	TBD	TBD
		"	15. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation.	Zero-cycle	P2	TBD	TBD	TBD

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
PL-2	PL-2	SYSTEM SECURITY AND PRIVACY PLANS (continued)	b. Distribute copies of the plans and communicate subsequent changes to the plans to organizational personnel with system security and privacy planning and plan implementation responsibilities; system developers; organizational personnel with information security and privacy responsibilities;	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Review the system security and privacy plans at least annually or when required due to system changes or modifications;	Zero-cycle	P2	TBD	TBD	TBD
		"	d. Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments; and	Zero-cycle	P2	TBD	TBD	TBD
		"	e. Protect the plans from unauthorized disclosure and modification.	Zero-cycle	P2	TBD	TBD	TBD
PL-4	PL-4	RULES OF BEHAVIOR	a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy;	Zero-cycle	P3	TBD	TBD	TBD
		"	b. Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system;	Zero-cycle	P3	TBD	TBD	TBD
		"	c. Review and update the rules of behavior at least annually; and	Zero-cycle	P3	TBD	TBD	TBD
		"	d. Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge annually, or when the rules are revised or updated.	Zero-cycle	P3	TBD	TBD	TBD
PL-4 (1)	PL-4 (1)	(1) RULES OF BEHAVIOR | SOCIAL MEDIA AND EXTERNAL SITE/APPLICATION USAGE RESTRICTIONS	Include in the rules of behavior, restrictions on:	Zero-cycle	P3	TBD	TBD	TBD
		"	(a) Use of social media, social networking sites, and external sites/applications;	Zero-cycle	P3	TBD	TBD	TBD
		"	(b) Posting organizational information on public websites; and	Zero-cycle	P3	TBD	TBD	TBD
		"	(c) Use of organization-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications.	Zero-cycle	P3	TBD	TBD	TBD
PL-8	PL-8	SECURITY AND PRIVACY ARCHITECTURES	a. Develop security and privacy architectures for the system that:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information;	Zero-cycle	P2	TBD	TBD	TBD
		"	2. Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals;	Zero-cycle	P2	TBD	TBD	TBD
		"	3. Describe how the architectures are integrated into and support the enterprise architecture; and	Zero-cycle	P2	TBD	TBD	TBD
		"	4. Describe any assumptions about, and dependencies on, external systems and services;	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Review and update the architectures at least annually or when changes to the system or its environment occur to reflect changes in the enterprise architecture; and	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and acquisitions.	Zero-cycle	P2	TBD	TBD	TBD
PL-9	PL-9	CENTRAL MANAGEMENT	The CJISSECPOL is centrally managed by the FBI CJIS ISO.	Zero-cycle	P4	TBD	TBD	TBD
PL-10	PL-10	BASELINE SELECTION	Select a control baseline for the system.	Zero-cycle	P3	TBD	TBD	TBD
PL-11	PL-11	BASELINE TAILORING	Tailor the selected control baseline by applying specified tailoring actions.	Zero-cycle	P3	TBD	TBD	TBD

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy Area 5-18 - Contingency Planning								
CP-1	CP-1	POLICY AND PROCEDURES	a. Develop, document, and disseminate to organizational personnel with contingency planning responsibilities:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. Agency-level contingency planning policy that:	Zero-cycle	P2	TBD	TBD	TBD
		"	(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Zero-cycle	P2	TBD	TBD	TBD
		"	(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and	Zero-cycle	P2	TBD	TBD	TBD
		"	2. Procedures to facilitate the implementation of the contingency planning policy and the associated contingency planning controls;	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Designate organizational personnel with information security responsibilities to manage the development, documentation, and dissemination of the contingency planning policy and procedures; and	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Review and update the current contingency planning:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. Policy annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI, or training simulations or exercises; and	Zero-cycle	P2	TBD	TBD	TBD
		"	2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI, or training simulations or exercises.	Zero-cycle	P2	TBD	TBD	TBD
CP-2	CP-2	CONTINGENCY PLAN	a. Develop a contingency plan for the system that:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. Identifies essential mission and business functions and associated contingency requirements;	Zero-cycle	P2	TBD	TBD	TBD
		"	2. Provides recovery objectives, restoration priorities, and metrics;	Zero-cycle	P2	TBD	TBD	TBD
		"	3. Addresses contingency roles, responsibilities, assigned individuals with contact information;	Zero-cycle	P2	TBD	TBD	TBD
		"	4. Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure;	Zero-cycle	P2	TBD	TBD	TBD
		"	5. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented;	Zero-cycle	P2	TBD	TBD	TBD
		"	6. Addresses the sharing of contingency information; and	Zero-cycle	P2	TBD	TBD	TBD
		"	7. Is reviewed and approved by agency head or their designee;	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Distribute copies of the contingency plan to organizational personnel with contingency planning or incident response duties;	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Coordinate contingency planning activities with incident handling activities;	Zero-cycle	P2	TBD	TBD	TBD
		"	d. Review the contingency plan for the system annually;	Zero-cycle	P2	TBD	TBD	TBD
		"	e. Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;	Zero-cycle	P2	TBD	TBD	TBD
		"	f. Communicate contingency plan changes to organizational personnel with contingency planning or incident response duties;	Zero-cycle	P2	TBD	TBD	TBD
		"	g. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; and	Zero-cycle	P2	TBD	TBD	TBD
		"	h. Protect the contingency plan from unauthorized disclosure and modification.	Zero-cycle	P2	TBD	TBD	TBD
CP-2 (1)	CP-2 (1)	(1) CONTINGENCY PLAN | COORDINATE WITH RELATED PLANS	Coordinate contingency plan development with organizational elements responsible for related plans.	Zero-cycle	P2	TBD	TBD	TBD
CP-2 (3)	CP-2 (3)	(3) CONTINGENCY PLAN | RESUME MISSION AND BUSINESS FUNCTIONS	Plan for the resumption of essential mission and business functions within twenty-four (24) hours of contingency plan activation.	Zero-cycle	P2	TBD	TBD	TBD

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CP-2 (8)	CP-2 (8)	(8) CONTINGENCY PLAN | IDENTIFY CRITICAL ASSETS	Identify critical system assets supporting essential mission and business functions.	Zero-cycle	P2	TBD	TBD	TBD
CP-3	CP-3	CONTINGENCY TRAINING	a. Provide contingency training to system users consistent with assigned roles and responsibilities:	Zero-cycle	P3	TBD	TBD	TBD
		"	1. Within thirty (30) days of assuming a contingency role or responsibility;	Zero-cycle	P3	TBD	TBD	TBD
		"	2. When required by system changes; and	Zero-cycle	P3	TBD	TBD	TBD
		"	3. Annually thereafter; and	Zero-cycle	P3	TBD	TBD	TBD
		"	b. Review and update contingency training content annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI, or training simulations or exercises.	Zero-cycle	P3	TBD	TBD	TBD
CP-4	CP-4	CONTINGENCY PLAN TESTING	a. Test the contingency plan for the system annually using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: checklists, walk-through and tabletop exercises, simulations (parallel or full interrupt), or comprehensive exercises.	Zero-cycle	P3	TBD	TBD	TBD
		"	b. Review the contingency plan test results; and	Zero-cycle	P3	TBD	TBD	TBD
		"	c. Initiate corrective actions, if needed.	Zero-cycle	P3	TBD	TBD	TBD
CP-4 (1)	CP-4 (1)	(1) CONTINGENCY PLAN TESTING | COORDINATE WITH RELATED PLANS	Coordinate contingency plan testing with organizational elements responsible for related plans.	Zero-cycle	P3	TBD	TBD	TBD
CP-6	CP-6	ALTERNATE STORAGE SITE	a. Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information; and	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Ensure that the alternate storage site provides controls equivalent to that of the primary site.	Zero-cycle	P2	TBD	TBD	TBD
CP-6 (1)	CP-6 (1)	(1) ALTERNATE STORAGE SITE | SEPARATION FROM PRIMARY SITE	Identify an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats.	Zero-cycle	P2	TBD	TBD	TBD
CP-6 (3)	CP-6 (3)	(3) ALTERNATE STORAGE SITE | ACCESSIBILITY	Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.	Zero-cycle	P2	TBD	TBD	TBD
CP-7	CP-7	ALTERNATE PROCESSING SITE	a. Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of operations for essential mission and business functions within the time period defined in the system contingency plan(s) when the primary processing capabilities are unavailable;	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Make available at the alternate processing site, the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery to the site within the organization-defined time period for transfer and resumption; and	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Provide controls at the alternate processing site that are equivalent to those at the primary site.	Zero-cycle	P2	TBD	TBD	TBD
CP-7 (1)	CP-7 (1)	(1) ALTERNATE PROCESSING SITE | SEPARATION FROM PRIMARY SITE	Identify an alternate processing site that is sufficiently separated from the primary processing site to reduce susceptibility to the same threats.	Zero-cycle	P2	TBD	TBD	TBD
CP-7 (2)	CP-7 (2)	(2) ALTERNATE PROCESSING SITE | ACCESSIBILITY	Identify potential accessibility problems to alternate processing sites in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.	Zero-cycle	P2	TBD	TBD	TBD
CP-7 (3)	CP-7 (3)	(3) ALTERNATE PROCESSING SITE | PRIORITY OF SERVICE	Develop alternate processing site agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives).	Zero-cycle	P2	TBD	TBD	TBD

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CP-8	CP-8	TELECOMMUNICATIONS SERVICES	Establish alternate telecommunications services, including necessary agreements to permit the resumption of system operations for essential mission and business functions within the time period as defined in the system contingency plan(s) when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.	Zero-cycle	P2	TBD	TBD	TBD
CP-8 (1)	CP-8 (1)	(1) TELECOMMUNICATIONS SERVICES | PRIORITY OF SERVICE PROVISIONS	(a) Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives); and	Zero-cycle	P2	TBD	TBD	TBD
		"	(b) Request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness if the primary and/or alternate telecommunications services are provided by a common carrier.	Zero-cycle	P2	TBD	TBD	TBD
CP-8 (2)	CP-8 (2)	(2) TELECOMMUNICATIONS SERVICES | SINGLE POINTS OF FAILURE	Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.	Zero-cycle	P2	TBD	TBD	TBD
CP-9	CP-9	SYSTEM BACKUP	a. Conduct backups of user-level information contained in operational systems for essential business functions as required by the contingency plans;	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Conduct backups of system-level information contained in the system as required by the contingency plans;	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Conduct backups of system documentation, including security- and privacy-related documentation as required by the contingency plans; and	Zero-cycle	P2	TBD	TBD	TBD
		"	d. Protect the confidentiality, integrity, and availability of backup information.	Zero-cycle	P2	TBD	TBD	TBD
CP-9 (1)	CP-9 (1)	(1) SYSTEM BACKUP | TESTING FOR RELIABILITY AND INTEGRITY	Test backup information as required by the contingency plans to verify media reliability and information integrity.	Zero-cycle	P2	TBD	TBD	TBD
CP-9 (8)	CP-9 (8)	(8) SYSTEM BACKUP | CRYPTOGRAPHIC PROTECTION	Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of CJI.	Zero-cycle	P2	TBD	TBD	TBD
CP-10	CP-10	SYSTEM RECOVERY AND RECONSTITUTION	Provide for the recovery and reconstitution of the system to a known state within the timeframe as required by the contingency plans after a disruption, compromise, or failure.	Zero-cycle	P2	TBD	TBD	TBD
CP-10 (2)	CP-10 (2)	(2) SYSTEM RECOVERY AND RECONSTITUTION | TRANSACTION RECOVERY	Implement transaction recovery for systems that are transaction-based.	Zero-cycle	P2	TBD	TBD	TBD

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy Area 5-19 - Risk Assessment								
RA-1	RA-1	POLICY AND PROCEDURES	a. Develop, document, and disseminate to organizational personnel with risk assessment responsibilities:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. Agency Level risk assessment policy that:	Zero-cycle	P2	TBD	TBD	TBD
		"	(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Zero-cycle	P2	TBD	TBD	TBD
		"	(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and	Zero-cycle	P2	TBD	TBD	TBD
		"	2. Procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls;	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Designate organizational personnel with security and privacy responsibilities to manage the development, documentation, and dissemination of the risk assessment policy and procedures; and	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Review and update the current risk assessment:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. Policy annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI; and	Zero-cycle	P2	TBD	TBD	TBD
		"	2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.	Zero-cycle	P2	TBD	TBD	TBD
RA-2	RA-2	SECURITY CATEGORIZATION	a. Categorize the system and information it processes, stores, and transmits;	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Document the security categorization results, including supporting rationale, in the security plan for the system; and	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Verify that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.	Zero-cycle	P2	TBD	TBD	TBD
RA-3	RA-3	RISK ASSESSMENT	a. Conduct a risk assessment, including:	Zero-cycle	P2	TBD	TBD	TBD
		"	1. Identifying threats to and vulnerabilities in the system;	Zero-cycle	P2	TBD	TBD	TBD
		"	2. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and	Zero-cycle	P2	TBD	TBD	TBD
		"	3. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information;	Zero-cycle	P2	TBD	TBD	TBD
		"	b. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments;	Zero-cycle	P2	TBD	TBD	TBD
		"	c. Document risk assessment results in risk assessment report;	Zero-cycle	P2	TBD	TBD	TBD
		"	d. Review risk assessment results at least quarterly;	Zero-cycle	P2	TBD	TBD	TBD
		"	e. Disseminate risk assessment results to organizational personnel with risk assessment responsibilities and organizational personnel with security and privacy responsibilities; and	Zero-cycle	P2	TBD	TBD	TBD
		"	f. Update the risk assessment at least quarterly or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.	Zero-cycle	P2	TBD	TBD	TBD
RA-5	RA-5	VULNERABILITY MONITORING AND SCANNING	a. Monitor and scan for vulnerabilities in the system and hosted applications at least monthly and when new vulnerabilities potentially affecting the system are identified and reported;	10/1/2024	P1	TBD	TBD	TBD
		"	b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:	10/1/2024	P1	TBD	TBD	TBD
		"	1. Enumerating platforms, software flaws, and improper configurations;	10/1/2024	P1	TBD	TBD	TBD
		"	2. Formatting checklists and test procedures; and	10/1/2024	P1	TBD	TBD	TBD
		"	3. Measuring vulnerability impact;	10/1/2024	P1	TBD	TBD	TBD

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
RA-5	RA-5	VULNERABILITY MONITORING AND SCANNING (continued)	c. Analyze vulnerability scan reports and results from vulnerability monitoring;	10/1/2024	P1	TBD	TBD	TBD
		"	d. Remediate legitimate vulnerabilities within the number of days listed;	10/1/2024	P1	TBD	TBD	TBD
		"	• Critical–15 days	10/1/2024	P1	TBD	TBD	TBD
		"	• High–30 days	10/1/2024	P1	TBD	TBD	TBD
		"	• Medium–60 days	10/1/2024	P1	TBD	TBD	TBD
		"	• Low–90 days; and	10/1/2024	P1	TBD	TBD	TBD
		"	e. Share information obtained from the vulnerability monitoring process and control assessments with organizational personnel with risk assessment, control assessment, and vulnerability scanning responsibilities to help eliminate similar vulnerabilities in other systems; and	10/1/2024	P1	TBD	TBD	TBD
		"	f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.	10/1/2024	P1	TBD	TBD	TBD
RA-5 (2)	RA-5 (2)	(2) VULNERABILITY MONITORING AND SCANNING | UPDATE VULNERABILITIES TO BE SCANNED	Update the system vulnerabilities to be scanned within 24 hours prior to running a new scan or when new vulnerabilities are identified and reported.	10/1/2024	P1	TBD	TBD	TBD
RA-5 (5)	RA-5 (5)	(5) VULNERABILITY MONITORING AND SCANNING | PRIVILEGED ACCESS	Implement privileged access authorization to information system components containing or processing CJI for vulnerability scanning activities requiring privileged access.	10/1/2024	P1	TBD	TBD	TBD
RA-5 (11)	RA-5 (11)	(11) VULNERABILITY MONITORING AND SCANNING | PUBLIC DISCLOSURE PROGRAM	Establish a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components.	10/1/2024	P1	TBD	TBD	TBD
RA-7	RA-7	RISK RESPONSE	Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.	Zero-cycle	P2	TBD	TBD	TBD
RA-9	RA-9	CRITICALITY ANALYSIS	Identify critical system components and functions by performing a criticality analysis for information system components containing or processing CJI at the planning, design, development, testing, implementation, and maintenance stages of the system development life cycle.	Zero-cycle	P2	TBD	TBD	TBD