



Requirements Companion Document to the FBI CJIS Security Policy Version 5.9

06/01/2020



Prepared by:
CJIS Information Security Officer

Recommended changes to version 5.8 of the *CJIS Security Policy* were approved by the Advisory Policy Board (APB) in 2019 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.

Effective October 1, 2014, Noncriminal Justice Agencies (NCJA) who had not previously been subject to CJIS Security Policy audit and whose only access to FBI CJIS data is for the purpose of civil fingerprint-based background checks or other noncriminal justice purposes, became subject to zero-cycle audits. ***The zero-cycle audits ended September 30, 2017.***

The “Summary of Changes” page lists the line numbers corresponding to requirements that were added, deleted, or changed from the previous version and are now reflected in the current version as well as a summary of the change(s). Within the document, modifications are highlighted in yellow for ease of location.

The document contains a “Requirement Priority Tier” column. This column lists the individual requirement tier of 1 or 2. Tier 1 requirements are indicated in **BLUE**. Tier 2 requirements are indicated in **GOLD**. Tier priorities are defined as indicated here:

- Tier 1 requirements must be met by a system before a CSO can approve connection to the state system.
- Tier 2 requirements must be met by the date indicated in the plan approved by the CSO.

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

Please refer questions or comments about this document or the current version of the *CJIS Security Policy* to your respective Information Security Officer, CJIS Systems Officer, or Compact Officer.

SUMMARY OF CHANGES

Version 5.9

Requirement No.	Change
541 – 553	The language in the main requirement statement for this range of requirements changed.

	Ver 5.8 Location and New Requirement	Ver 5.9 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
Security Policy Sections 1 - 4 (Introduction, Approach, Roles & Responsibilities, and CJI/PII)								
1			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,....	1	Agency	Agency	Agency
2	1.3	1.3	"	...and local policy may augment, or increase the standards, but shall not detract from the CJIS Security Policy standards.	1	Agency	Agency	Agency
3			"	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.	2	Agency	Agency	Agency
4			"	The policies and procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.	1	Agency	Agency	Agency
5	3.2.1	3.2.1	CJIS Systems Agencies (CSA)	The head of each CSA shall appoint a CJIS Systems Officer (CSO).	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
6			"	Such decisions shall be documented and kept current.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
7	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.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
8	3.2.2(1)	3.2.2(1)	"	The CSO shall set, maintain, and enforce the following: 1. Standards for the selection, supervision, and separation of personnel who have access to CJI.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
9			"	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.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
10			"	a. Ensure appropriate use, enforce system discipline, and ensure CJIS Division operating procedures are followed by all users of the respective services and information.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
11	3.2.2(2)	3.2.2(2)	"	b. Ensure state/federal agency compliance with policies approved by the APB and adopted by the FBI.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
12			"	c. Ensure the appointment of the CSA ISO and determine the extent of authority to the CSA ISO.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
13			"	d. Ensure the designation of a Terminal Agency Coordinator (TAC) within each agency with device access to CJIS systems.	1	Agency	Agency	Agency
14			"	e. Ensure each agency having access to CJI has someone designated as the Local Agency Security Officer (LASO).	1	Agency	Agency	Agency
15	3.2.2(2)	3.2.2(2)	"	f. Ensure the LASO receives enhanced security awareness training (ref. Section 5.2).	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
16			"	g. Approve access to FBI CJIS systems.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
17	3.2.2(2)	3.2.2(2)	"	h. Assume ultimate responsibility for managing the security of CJIS systems within their state and/or agency.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
18			"	i. Perform other related duties outlined by the user agreements with the FBI CJIS Division.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
19	3.2.3(3)	3.2.3(3)	"	3. Outsourcing of Criminal Justice Functions a. Responsibility for the management of the approved security requirements shall remain with the CJA.	1	Agency	Agency	Agency
20			"	b. Responsibility for the management control of network security shall remain with the CJA.	1	Agency	Agency	Agency
21	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.	1	Agency	Agency	Agency

	Ver 5.8 Location and New Requirement	Ver 5.9 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
22	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.	1	Agency	Agency	Agency
			"	The AC shall:				
23			"	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.	1	Agency	Agency	Agency
24			"	2. Participate in related meetings and provide input and comments for system improvement.	2	Agency	Agency	Agency
25			"	3. Receive information from the CGA (e.g., system updates) and disseminate it to appropriate Contractor employees.	1	Agency	Agency	Agency
26			"	4. Maintain and update manuals applicable to the effectuation of the agreement, and provide them to the Contractor.	2	Agency	Agency	Agency
27			"	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).	1	Agency	Agency	Agency
28	3.2.7	3.2.7	"	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.	1	Agency	Agency	Agency
29			"	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.	2	Agency	Agency	Agency
30			"	8. Where appropriate, ensure compliance by the Contractor with NCIC validation requirements.	1	Agency	Agency	Agency
31			"	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.	1	Agency	Agency	Agency
32	3.2.7	3.2.7	"	10. Any other responsibility for the AC promulgated by the FBI.	1	Agency	Agency	Agency
			CJIS System Agency Information Security Officer (CSA ISO)	The CSA ISO shall:				
33			"	1. Serve as the security point of contact (POC) to the FBI CJIS Division ISO.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
34	3.2.8	3.2.8	"	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.	2	CJIS/CSO	CJIS/CSO	CJIS/CSO
35			"	3. Document and provide assistance for implementing the security-related controls for the Interface Agency and its users.	2	CJIS/CSO	CJIS/CSO	CJIS/CSO
36			"	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.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
	3.2.9	3.2.9	Local Agency Security Officer (LASO)	Each LASO shall:				

	Ver 5.8 Location and New Requirement	Ver 5.9 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
37			Local Agency Security Officer (LASO) (continued)	1. Identify who is using the CSA approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.	1	Agency	Agency	Agency
38			"	2. Identify and document how the equipment is connected to the state system.	1	Agency	Agency	Agency
39	3.2.9	3.2.9	"	3. Ensure that personnel security screening procedures are being followed as stated in this policy.	1	Agency	Agency	Agency
40			"	4. Ensure the approved and appropriate security measures are in place and working as expected.	1	Agency	Agency	Agency
41			"	5. Support policy compliance and ensure CSA ISO is promptly informed of security incidents.	1	Agency	Agency	Agency
			FBI CJIS Division Information Security Officer (FBI CJIS ISO)	The FBI CJIS ISO shall:				
42			"	1. Maintain the CJIS Security Policy.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
43			"	2. Disseminate the FBI Director approved CJIS Security Policy.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
44			"	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.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
45	3.2.10	3.2.10	"	4. Serve as a point-of-contact (POC) for computer incident notification and distribution of security alerts to the CSOs and ISOs.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
46			"	5. Assist with developing audit compliance guidelines as well as identifying and reconciling security-related issues.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
47			"	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.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
48	3.2.10	3.2.10	"	7. Maintain a security policy resource center (SPRC) on FBI.gov and keep the CSOs and ISOs updated on pertinent information.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
49	3.2.12	3.2.12	Compact Officer	Pursuant to the National Crime Prevention and Privacy Compact, each party state	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
50				...Compact Officer who shall ensure that Compact provisions and rules, procedure	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
51	4.2.1	4.2.1	Proper Access, Use, and Dissemination of CHRl	The Ill shall be accessed only for an authorized purpose.	1	Agency	Agency	Agency
52			"	Further, CHRl shall only be used for an authorized purpose consistent with the purpose for which Ill was accessed.	1	Agency	Agency	Agency
53			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 Ill described in Title 28, Part 20, CFR, and the NCIC Operating Manual.	1	Agency	Agency	Agency
			"	The restricted files, which shall be protected as CHRl, are as follows:				
54			"	1. Gang File	1	Agency	Agency	Agency
55			"	2. Known or Appropriately Suspected Terrorist File	1	Agency	Agency	Agency
56			"	3. Supervised Release File	1	Agency	Agency	Agency
57	4.2.2	4.2.2	"	4. National Sex Offender Registry File	1	Agency	Agency	Agency
58			"	5. Historical Protection Order File of the NCIC	1	Agency	Agency	Agency
59			"	6. Identity Theft File	1	Agency	Agency	Agency
60			"	7. Protective Interest File	1	Agency	Agency	Agency
61			"	8. Person With Information [PWI] data in the Missing Person Files	1	Agency	Agency	Agency
62			"	9. Violent Person File	1	Agency	Agency	Agency
63			"	10. NICS Denied Transaction File	1	Agency	Agency	Agency
64	4.2.3.2	4.2.3.2	For Other Authorized Purposes	Non-restricted files information shall not be disseminated commercially.	1	Agency	Agency	Agency

	Ver 5.8 Location and New Requirement	Ver 5.9 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
65	4.2.3.2	4.2.3.2	For Other Authorized Purposes (continued)	Agencies shall not disseminate restricted files information for purposes other than law enforcement.	1	Agency	Agency	Agency
66	4.2.4	4.2.4	Storage	When CHR1 is stored, agencies shall establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of the information.	1	Agency	Agency	Agency
67			"	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.	1	Agency	Agency	Agency
68	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.	1	Agency	Agency	Agency
69	4.3	4.3	Personally Identifiable Information (PII)	PII shall be extracted from CJI for the purpose of official business only.	1	Agency	Agency	Agency
70			"	Agencies shall develop policies, based on state and local privacy rules, to ensure appropriate controls are applied when handling PII extracted from CJI.	1	Agency	Agency	Agency

	Ver 5.8 Location and New Requirement	Ver 5.9 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy Area 1 - Information Exchange Agreements								
71	5.1	5.1	Policy Area 1: Information Exchange Agreements	The information shared through communication mediums shall be protected with appropriate security safeguards.	1	Agency	Agency	Agency
72			Information Exchange	Before exchanging CJ, agencies shall put formal agreements in place that specify security controls.	1	Agency	Agency	Agency
73	5.1.1	5.1.1	"	Information exchange agreements for agencies sharing CJ data that is sent to and/or received from the FBI CJIS shall specify the security controls and conditions described in this document.	1	Agency	Agency	Agency
74			"	Information exchange agreements shall be supported by documentation committing both parties to the terms of information exchange.	1	Agency	Agency	Agency
75			"	Law Enforcement and civil agencies shall have a local policy to validate a requestor of CJ as an authorized recipient before disseminating CJ.	1	Agency	Agency	Agency
76	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.	1	Agency	Agency	Agency
77			"	Using the requirements in this policy as a starting point, the procedures shall apply to the handling, processing, storing, and communication of CJ.	1	Agency	Agency	Agency
78			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.	1	Agency	Agency	Agency
79	5.1.1.2	5.1.1.2	"	This agreement shall include the standards and sanctions governing utilization of CJIS systems.	1	Agency	Agency	Agency
80			"	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.	1	Agency	Agency	Agency
81			"	All user agreements with the FBI CJIS Division shall be coordinated with the CSA head.	1	Agency	Agency	Agency
82			Criminal Justice Agency User Agreements	Any CJA receiving access to FBI CJ shall enter into a signed written agreement with the appropriate signatory authority of the CSA providing the access.	1	Agency	Agency	Agency
83			"	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.	1	Agency	Agency	Agency
			"	These agreements shall include:				
84			"	1. Audit.	1	Agency	Agency	Agency
85			"	2. Dissemination.	1	Agency	Agency	Agency
86	5.1.1.3	5.1.1.3	"	3. Hit confirmation.	1	Agency	Agency	Agency
87			"	4. Logging.	1	Agency	Agency	Agency
88			"	5. Quality Assurance (QA).	1	Agency	Agency	Agency
89			"	6. Screening (Pre-Employment).	1	Agency	Agency	Agency
90			"	7. Security.	1	Agency	Agency	Agency
91			"	8. Timeliness.	1	Agency	Agency	Agency
92			"	9. Training.	1	Agency	Agency	Agency
93			"	10. Use of the system.	1	Agency	Agency	Agency
94			"	11. Validation.	1	Agency	Agency	Agency
95	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 CJ.	1	Agency	Agency	Agency
96			"	Access shall be permitted when such designation is authorized pursuant to Executive Order, statute, regulation, or inter-agency agreement.	1	Agency	Agency	Agency

	Ver 5.8 Location and New Requirement	Ver 5.9 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
97	5.1.1.4	5.1.1.4	Inter-Agency and Management Control Agreements (continued)	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.	1	Agency	Agency	Agency
98			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....	1	Both	Both	Both
99			"	...and shall be subject to the same extent of audit review as are local user agencies.	1	Both	Both	Both
100			"	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.	1	Both	Both	Both
101			"	Modifications to the CJIS Security Addendum shall be enacted only by the FBI.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
102			"	1. Private contractors designated to perform criminal justice functions for a CJA shall be eligible for access to CJI.	1	Agency	Agency	Agency
103	5.1.1.5	5.1.1.5	"	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.	1	Agency	Agency	Agency
104			"	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).	1	Agency	Agency	Agency
105			"	2. Private contractors designated to perform criminal justice functions on behalf of a NCJA (government) shall be eligible for access to CJI.	1	Agency	Agency	Agency
106			"	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.	1	Agency	Agency	Agency
107			"	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).	1	Agency	Agency	Agency
108			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.	1	Agency	Agency	Agency
109			"	Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General.	1	Agency	Agency	Agency
110			"	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.	1	Agency	Agency	Agency
111	5.1.1.6	5.1.1.6	"	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.	1	Agency	Agency	Agency
112			"	Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General.	1	Agency	Agency	Agency
113			"	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.	1	Agency	Agency	Agency
114			"	All NCJAs accessing CJI shall be subject to all pertinent areas of the CJIS Security Policy (see appendix J for supplemental guidance).	1	Agency	Agency	Agency

	Ver 5.8 Location and New Requirement	Ver 5.9 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
115	5.1.1.6	5.1.1.6	Agency User Agreements (continued)	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.	1	Agency	Agency	Agency
116			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.	1	Agency	Agency	Agency
117			"	Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General.	1	Agency	Agency	Agency
118	5.1.1.7	5.1.1.7	"	All Channelers accessing CJI shall be subject to the terms and conditions described in the Compact Council Security and Management Control Outsourcing Standard.	1	Agency	Agency	Agency
119			"	Each Channeler that directly accesses CJI shall also allow the FBI to conduct periodic penetration testing.	1	Agency	Agency	Agency
120			"	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....	1	Agency	Agency	Agency
121			"	...and shall be subject to the same extent of audit review as are local user agencies.	1	Agency	Agency	Agency
122			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.	1	Agency	Agency	Agency
123	5.1.1.8	5.1.1.8	"	Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General.	1	Agency	Agency	Agency
124			"	All contractors accessing CJI shall be subject to the terms and conditions described in the Compact Council Outsourcing Standard for Non-Channelers.	1	Agency	Agency	Agency
125			"	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....	1	Agency	Agency	Agency
126	5.1.1.8	5.1.1.8	"	...and shall be subject to the same extent of audit review as are local user agencies.	1	Agency	Agency	Agency
127	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.	1	Agency	Agency	Agency
128	5.1.2	5.1.2	"	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.	1	Agency	Agency	Agency
129			"	The incident reporting/response process used by the service provider shall conform to the incident reporting/response specifications provided in this policy.	1	Agency	Agency	Agency
130	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.	1	Agency	Agency	Agency
131			"	Evaluation of the risks to the agency shall be undertaken based on the criticality of the data, system, and the impact of the change.	1	Agency	Agency	Agency
132	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.	1	Agency	Agency	Agency
133	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.	1	Agency	Agency	Agency

	Ver 5.8 Location and New Requirement	Ver 5.9 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy Area 2 - Security Awareness Training								
134	5.2.1	5.2.1	Basic Security Awareness Training	Basic security awareness training shall be required within six months of initial assignment and biennially thereafter, for all personnel who have access to CJJ to include all personnel who have unescorted access to a physically secure location.	1	Both	Both	Both
135			Level One Security Awareness Training	At a minimum, the following topics shall be addressed as baseline security awareness training for all personnel who have access to a physically secure location: 1. Individual responsibilities and expected behavior with regard to being in the vicinity of CJJ usage and/or terminals. 2. Implications of noncompliance. 3. Incident response (Identify points of contact and individual actions). 4. Visitor control and physical access to spaces—discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity, etc.	1	Both	Both	Both
136	5.2.1.1	5.2.1.1	"	1. Individual responsibilities and expected behavior with regard to being in the vicinity of CJJ usage and/or terminals.	1	Both	Both	Both
137			"	2. Implications of noncompliance.	1	Both	Both	Both
138			"	3. Incident response (Identify points of contact and individual actions).	1	Both	Both	Both
			"	4. Visitor control and physical access to spaces—discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity, etc.	1	Both	Both	Both
			Level Two Security Awareness Training	In addition to 5.2.1.1 above, the following topics, at a minimum, shall be addressed as baseline security awareness training for all authorized personnel with access to CJJ: 1. Media Protection. 2. Protect information subject to confidentiality concerns — hardcopy through destruction. 3. Proper handling and marking of C.J.I. 4. Threats, vulnerabilities, and risks associated with handling of C.J.I. 5. Social engineering. 6. Dissemination and destruction.	1	Both	Both	Both
139			"	1. Media Protection.	1	Both	Both	Both
140	5.2.1.2	5.2.1.2	"	2. Protect information subject to confidentiality concerns — hardcopy through destruction.	1	Both	Both	Both
141			"	3. Proper handling and marking of C.J.I.	1	Both	Both	Both
142			"	4. Threats, vulnerabilities, and risks associated with handling of C.J.I.	1	Both	Both	Both
143			"	5. Social engineering.	1	Both	Both	Both
144			"	6. Dissemination and destruction.	1	Both	Both	Both
			Level Three Security Awareness Training	In addition to 5.2.1.1 and 5.2.1.2 above, the following topics, at a minimum, shall be addressed as baseline security awareness training for all authorized personnel with both physical and logical access to CJJ: 1. Rules that describe responsibilities and expected behavior with regard to information system usage. 2. Password usage and management—including creation, frequency of changes, and protection. 3. Protection from viruses, worms, Trojan horses, and other malicious code. 4. Unknown e-mail/attachments. 5. Web usage—allowed versus prohibited; monitoring of user activity. 6. Spam. 7. Physical Security—increases in risks to systems and data. 8. Handheld device security issues—address both physical and wireless security issues. 9. Use of encryption and the transmission of sensitive/confidential information over the Internet—address agency policy, procedures, and technical contact for assistance. 10. Laptop security—address both physical and information security issues. 11. Personally owned equipment and software—state whether allowed or not (e.g., copyrights). 12. Access control issues—address least privilege and separation of duties. 13. Individual accountability—explain what this means in the agency. 14. Use of acknowledgement statements—passwords, access to systems and data, personal use and gain.	1	Both	Both	Both
145			"	1. Rules that describe responsibilities and expected behavior with regard to information system usage.	1	Both	Both	Both
146			"	2. Password usage and management—including creation, frequency of changes, and protection.	1	Both	Both	Both
147			"	3. Protection from viruses, worms, Trojan horses, and other malicious code.	1	Both	Both	Both
148			"	4. Unknown e-mail/attachments.	1	Both	Both	Both
149			"	5. Web usage—allowed versus prohibited; monitoring of user activity.	1	Both	Both	Both
150			"	6. Spam.	1	Both	Both	Both
151	5.2.1.3	5.2.1.3	"	7. Physical Security—increases in risks to systems and data.	1	Both	Both	Both
152			"	8. Handheld device security issues—address both physical and wireless security issues.	1	Both	Both	Both
153			"	9. Use of encryption and the transmission of sensitive/confidential information over the Internet—address agency policy, procedures, and technical contact for assistance.	1	Both	Both	Both
154			"	10. Laptop security—address both physical and information security issues.	1	Both	Both	Both
155			"	11. Personally owned equipment and software—state whether allowed or not (e.g., copyrights).	1	Both	Both	Both
156			"	12. Access control issues—address least privilege and separation of duties.	1	Both	Both	Both
157			"	13. Individual accountability—explain what this means in the agency.	1	Both	Both	Both
158			"	14. Use of acknowledgement statements—passwords, access to systems and data, personal use and gain.	1	Both	Both	Both

	Ver 5.8 Location and New Requirement	Ver 5.9 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
159			Level Three Security Awareness Training (continued)	15. Desktop security—discuss use of screensavers, restricting visitors' view of information on screen (preventing/limiting "shoulder surfing"), battery backup devices, allowed access to systems.	1	Both	Both	Both
160	5.2.1.3	5.2.1.3	"	16. Protect information subject to confidentiality concerns—in systems, archived, on backup media, and until destroyed.	1	Both	Both	Both
161			"	17. Threats, vulnerabilities, and risks associated with accessing CJIS Service systems and services.	1	Both	Both	Both
162			Level Four Security Awareness Training	In addition to 5.2.1.1, 5.2.1.2 and 5.2.1.3 above, the following topics at a minimum shall be addressed as baseline security awareness training for all Information Technology personnel (system administrators, security administrators, network administrators, etc.):				
163	5.2.1.4	5.2.1.4	"	1. Protection from viruses, worms, Trojan horses, and other malicious code—scanning, updating definitions.	1	Both	Both	Both
164			"	2. Data backup and storage—centralized or decentralized approach.	1	Both	Both	Both
165			"	3. Timely application of system patches—part of configuration management.	1	Both	Both	Both
166			"	4. Access control measures.	1	Both	Both	Both
167			LASO Training	5. Network infrastructure protection measures.	1	Both	Both	Both
168			"	LASO training shall be required prior to assuming duties but no later than six months after initial assignment and ...	1	Both	Both	Both
169	5.2.2	5.2.2	"	... and annually thereafter.				
170			"	At a minimum, the following topics shall be addressed as enhanced security awareness training for a LASO:	1	Both	Both	Both
171			"	1. The roles and responsibilities listed in CJIS Security Policy Section 3.2.9.	1	Both	Both	Both
172			"	2. Additional state/local/federal agency LASO roles and responsibilities.	1	Both	Both	Both
173			"	3. Summary of audit findings from previous state audits of local agencies.	1	Both	Both	Both
			"	4. Findings from the last FBI CJIS Division audit of the CSA.	1	Both	Both	Both
			"	5. Most recent changes to the CJIS Security Policy.	1	Both	Both	Both
174	5.2.3	5.2.3	Security Training Records	Records of individual basic security awareness training and specific information system security training shall be:	1	Both	Both	Both
175				- documented	1	Both	Both	Both
176				- kept current	1	Both	Both	Both
				- maintained by the CSO/SIB/Compact Officer				

	Ver 5.8 Location and New Requirement	Ver 5.9 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy Area 3 - Incident Response								
177			Policy Area 3: Incident Response	To ensure protection of CJI, agencies shall: (i) establish operational incident handling procedures that include adequate preparation, detection, analysis, containment, recovery, and user response activities....	1	Both	Both	Both
178	5.3	5.3	"	...(ii) track, document, and report incidents to appropriate agency officials and/or authorities.	1	Both	Both	Both
179			"	ISOs have been identified as the POC on security-related issues for their respective agencies and shall ensure LASOs institute the CSA incident response reporting procedures at the local level.	1	Both	Both	Both
180			Reporting Security Events	The agency shall promptly report incident information to appropriate authorities.	1	Both	Both	Both
181			"	Security events, including identified weaknesses associated with the event, shall be communicated in a manner allowing timely corrective action to be taken.	1	Both	Both	Both
182			"	Formal event reporting and escalation procedures shall be in place.	1	Both	Both	Both
183	5.3.1	5.3.1	"	Wherever feasible, the agency shall employ automated mechanisms to assist in the reporting of security incidents.	2	Both	Both	Both
184			"	All employees, contractors and third party users shall be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of agency assets and are required to report any security events and weaknesses as quickly as possible to the designated point of contact.	2	Both	Both	Both
			FBI CJIS Division Responsibilities	The FBI CJIS Division shall:				
185			"	1. Manage and maintain the CJIS Division's Computer Security Incident Response Capability (CSIRC).	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
186			"	2. Serve as a central clearinghouse for all reported intrusion incidents, security alerts, bulletins, and other security-related material.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
187	5.3.1.1.1	5.3.1.1.1	"	3. Ensure additional resources for all incidents affecting FBI CJIS Division controlled systems as needed.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
188			"	4. Disseminate prompt advisories of system threats and operating system vulnerabilities via the security policy resource center on FBI.gov, to include but not limited to: Product Security Bulletins, Virus Bulletins, and Security Clips.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
189			"	5. Track all reported incidents and/or trends.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
190			"	6. Monitor the resolution of all incidents.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
			CSA ISO Responsibilities	The CSA ISO shall:				
191	5.3.1.1.2	5.3.1.1.2	"	1. Assign individuals in each state, federal, and international law enforcement organization to be the primary point of contact for interfacing with the FBI CJIS Division concerning incident handling and response.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
192			"	2. Identify individuals who are responsible for reporting incidents within their area of responsibility.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
193			"	3. Collect incident information from those individuals for coordination and sharing among other organizations that may or may not be affected by the incident.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
194	5.3.1.1.2	5.3.1.1.2	"	4. Develop, implement, and maintain internal incident response procedures and coordinate those procedures with other organizations that may or may not be affected.	2	CJIS/CSO	CJIS/CSO	CJIS/CSO
195			"	5. Collect and disseminate all incident-related information received from the Department of Justice (DOJ), FBI CJIS Division, and other entities to the appropriate local law enforcement POCs within their area.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
196			"	6. Act as a single POC for their jurisdictional area for requesting incident response assistance.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO

	Ver 5.8 Location and New Requirement	Ver 5.9 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
197	5.3.2	5.3.2	Management of Security Incidents	A consistent and effective approach shall be applied to the management of security incidents.	1	Both	Both	Both
198			"	Responsibilities and procedures shall be in place to handle security events and weaknesses effectively once they have been reported.	1	Both	Both	Both
199	5.3.2.1	5.3.2.1	Incident Handling	The agency shall implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.	1	Both	Both	Both
200			"	Wherever feasible, the agency shall employ automated mechanisms to support the incident handling process.	2	Both	Both	Both
201	5.3.2.2	5.3.2.2	Collection of Evidence	Where a follow-up action against a person or agency after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).	1	Both	Both	Both
202	5.3.3	5.3.3	Incident Response Training	The agency shall ensure general incident response roles responsibilities are included as part of required security awareness training.	2	Both	Both	Both
203			Incident Monitoring	The agency shall track and document security incidents on an ongoing basis.	1	Both	Both	Both
204	5.3.4	5.3.4	"	The CSA ISO shall maintain completed security incident reporting forms until the subsequent FBI triennial audit or until legal action (if warranted) is complete (whichever time-frame is greater).	2	Both	Both	Both

	Ver 5.8 Location and New Requirement	Ver 5.9 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy Area 4 - Auditing and Accountability								
205			Policy Area 4: Auditing and Accountability	Agencies shall implement audit and accountability controls to increase the probability of authorized users conforming to a prescribed pattern of behavior.	1	Both	Both	Service Provider
206	5.4	5.4	"	Agencies shall carefully assess the inventory of components that compose their information systems to determine which security controls are applicable to the various components.	1	Both	Both	Service Provider
207			Auditable Events and Content (Information Systems)	The agency's information system shall generate audit records for defined events.	1	Both	Both	Service Provider
208			"	The agency shall specify which information system components carry out auditing activities.	1	Both	Both	Service Provider
209	5.4.1	5.4.1	"	The agency's information system shall produce, at the application and/or operating system level, audit records containing sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.	1	Both	Both	Service Provider
210			"	The agency shall periodically review and update the list of agency-defined auditable events.	2	Both	Both	Service Provider
211			"	In the event an agency does not use an automated system, manual recording of activities shall still take place.	1	Both	Both	Service Provider
			Events	The following events shall be logged:				
212			"	1. Successful and unsuccessful system log-on attempts.	1	Both	Both	Service Provider
213			"	2. Successful and unsuccessful attempts to access, create, write, delete or change permission on a user account, file, directory or other system resource.	1	Both	Both	Service Provider
214	5.4.1.1	5.4.1.1	"	3. Successful and unsuccessful attempts to change account passwords.	1	Both	Both	Service Provider
215			"	4. Successful and unsuccessful actions by privileged accounts.	1	Both	Both	Service Provider
216			"	5. Successful and unsuccessful attempts for users to access, modify, or destroy the audit log file.	1	Both	Both	Service Provider
			Content	The following content shall be included with every audited event:				
217			"	1. Date and time of the event.	1	Both	Both	Service Provider
218			"	2. The component of the information system (e.g., software component, hardware component) where the event occurred.	1	Both	Both	Service Provider
219	5.4.1.1.1	5.4.1.1.1	"	3. Type of event.	1	Both	Both	Service Provider
220			"	4. User/subject identity.	1	Both	Both	Service Provider
221			"	5. Outcome (success or failure) of the event.	1	Both	Both	Service Provider
222	5.4.2	5.4.2	Response to Audit Processing Failures	The agency's information system shall provide alerts to appropriate agency officials in the event of an audit processing failure.	2	Both	Both	Both
223			Audit Monitoring, Analysis, and Reporting	The responsible management official shall designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions.	2	Both	Both	Both
224	5.4.3	5.4.3	"	Audit review/analysis shall be conducted at a minimum once a week.	2	Both	Both	Both
225			"	The agency shall increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to agency operations, agency assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.	2	Both	Both	Both

	Ver 5.8 Location and New Requirement	Ver 5.9 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
226			Time Stamps	The agency's information system shall provide time stamps for use in audit record generation.	2	Both	Both	Service Provider
227	5.4.4	5.4.4	"	The time stamps shall include the date and time values generated by the internal system clocks in the audit records.	2	Both	Both	Service Provider
228			"	The agency shall synchronize internal information system clocks on an annual basis.	2	Both	Both	Service Provider
229	5.4.5	5.4.5	Protection of Audit Information	The agency's information system shall protect audit information and audit tools from modification, deletion and unauthorized access.	1	Both	Both	Service Provider
230			Audit Record Retention	The agency shall retain audit records for at least one (1) year.	1	Both	Both	Service Provider
231	5.4.6	5.4.6	"	Once the minimum retention time period has passed, the agency shall continue to retain audit records until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes.	1	Both	Both	Service Provider
232			Logging NCIC and III Transactions	A log shall be maintained for a minimum of one (1) year on all NCIC and III transactions.	1	Both	Both	Service Provider
233			"	The III portion of the log shall clearly identify both the operator and the authorized receiving agency.	1	Agency	Agency	Agency
234	5.4.7	5.4.7	"	III logs shall also clearly identify the requester and the secondary recipient.	1	Agency	Agency	Agency
235			"	The identification on the log shall take the form of a unique identifier that shall remain unique to the individual requester and to the secondary recipient throughout the minimum one-year retention period.	1	Agency	Agency	Agency

	Ver 5.8 Location and New Requirement	Ver 5.9 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy Area 5 - Access Control								
236			Account Management	The agency shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts.	1	Agency	Both	Both
237			"	The agency shall validate information system accounts at least annually and...	1	Agency	Both	Both
238			"	...and shall document the validation process.	2	Agency	Both	Both
239			"	The agency shall identify authorized users of the information system and specify access rights/privileges.	1	Agency	Both	Both
240	5.5.1	5.5.1	"	The agency shall grant access to the information system based on:				
241			"	1. Valid need-to-know/need-to-share that is determined by assigned official duties.	1	Agency	Both	Both
242			"	2. Satisfaction of all personnel security criteria.	1	Agency	Both	Both
243			"	The agency responsible for account creation shall be notified when:				
244			Access Enforcement	1. A user's information system usage or need-to-know or need-to-share changes.	1	Agency	Both	Both
245			"	2. A user is terminated or transferred or associated accounts are removed, disabled, or otherwise secured.	1	Agency	Both	Both
246	5.5.2	5.5.2	"	The information system shall enforce assigned authorizations for controlling access to the system and contained information.	1	Agency	Both	Both
247			Least Privilege	The information system controls shall restrict access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel.	1	Agency	Both	Both
248			"	Access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) shall be employed by agencies to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system.	1	Agency	Both	Both
249	5.5.2.1	5.5.2.1	"	The agency shall approve individual access privileges and...	1	Agency	Both	Both
250			"	...and shall enforce physical and logical access restrictions associated with changes to the information system; and generate, retain, and review records reflecting all such changes.	1	Agency	Both	Both
251			"	The agency shall enforce the most restrictive set of rights/privileges or access needed by users for the performance of specified tasks.	1	Agency	Both	Both
252			System Access Control	The agency shall implement least privilege based on specific duties, operations, or information systems as necessary to mitigate risk to CJI.	1	Agency	Both	Both
253	5.5.2.2	5.5.2.2	"	Logs of access privilege changes shall be maintained for a minimum of one year or at least equal to the agency's record retention policy – whichever is greater.	2	Agency	Both	Both
254			"	Access control mechanisms to enable access to CJI shall be restricted by object (e.g., data set, volumes, files, records) including the ability to read, write, or delete the objects.	2	Agency	Both	Both
255			"	Access controls shall be in place and operational for all IT systems to:				
			"	1. Prevent multiple concurrent active sessions for one user identification, for those applications accessing CJI, unless the agency grants authority based upon operational business needs.	2	Agency	Both	Both
			"	(1. continued) Agencies shall document the parameters of the operational business needs for multiple concurrent active sessions.	2	Agency	Both	Both
			"	2. Ensure that only authorized personnel can add, change, or remove component devices, dial-up connections, and remove or alter programs.	1	Agency	Both	Both

	Ver 5.8 Location and New Requirement	Ver 5.9 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
			Access Control Criteria	Agencies shall control access to CJI based on one or more of the following: 1. Job assignment or function (i.e., the role) of the user seeking access. 2. Physical location. 3. Logical location. 4. Network addresses (e.g., users from sites within a given agency may be permitted greater access than those from outside). 5. Time-of-day and day-of-week/month restrictions.				
256			"		1	Agency	Both	Both
257			"		1	Agency	Both	Both
258	5.5.2.3	5.5.2.3	"		1	Agency	Both	Both
259			"		1	Agency	Both	Both
260			"		1	Agency	Both	Both
			Access Control Mechanisms	When setting up access controls, agencies shall use one or more of the following mechanisms: 1. Access Control Lists (ACLs). ACLs are a register of users (including groups, machines, processes) who have been given permission to use a particular object (system resource) and the types of access they have been permitted. 2. Resource Restrictions. Access to specific functions is restricted by never allowing users to request information, functions, or other resources for which they do not have access. Three major types of resource restrictions are: menus, database views, and network devices. 3. Encryption. Encrypted information can only be decrypted, and therefore read, by those possessing the appropriate cryptographic key. While encryption can provide strong access control, it is accompanied by the need for strong key management. If encryption of stored information is employed as an access enforcement mechanism, the cryptography used is Federal Information Processing Standards (FIPS) 140-2 (as amended) compliant (see section 5.10.1.1.2 for encryption requirements). 4. Application Level. In addition to controlling access at the information system level, access enforcement mechanisms are employed at the application level to provide increased information security for the agency. Where technically feasible, the system shall enforce a limit of no more than 5 consecutive invalid access attempts by a user (attempting to access CJI or systems with access to CJI). The system shall automatically lock the account/node for a 10 minute time period unless released by an administrator. The information system shall display an approved system use notification message, before granting access, informing potential users of various usages and monitoring rules. The system use notification message shall , at a minimum, provide the following information: 1. The user is accessing a restricted information system. 2. System usage may be monitored, recorded, and subject to audit. 3. Unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties. 4. Use of the system indicates consent to monitoring and recording. The system use notification message shall provide appropriate privacy and security notices (based on associated privacy and security policies or summaries) and... ...and remain on the screen until the user acknowledges the notification and takes explicit actions to log on to the information system. Privacy and security policies shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.				
261			"		1	Agency	Both	Both
262			"		1	Agency	Both	Both
263	5.5.2.4	5.5.2.4	"		1	Agency	Both	Both
264			"		1	Agency	Both	Both
265	5.5.3	5.5.3	Unsuccessful Login Attempts		2	Agency	Both	Both
266			"		2	Agency	Both	Both
267			System Use Notification		2	Agency	Both	Both
268			"		2	Agency	Both	Both
269			"		2	Agency	Both	Both
270	5.5.4	5.5.4	"		2	Agency	Both	Both
271			"		2	Agency	Both	Both
272			"		2	Agency	Both	Both
273			"		2	Agency	Both	Both
274			"		2	Agency	Both	Both

	Ver 5.8 Location and New Requirement	Ver 5.9 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
275			Session Lock	The information system shall prevent further access to the system by initiating a session lock after a maximum of 30 minutes of inactivity, and....	2	Agency	Both	Both
276	5.5.5	5.5.5	"	...and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures.	2	Agency	Both	Both
277			"	Users shall directly initiate session lock mechanisms to prevent inadvertent viewing when a device is unattended.	2	Agency	Both	Both
278			Remote Access	The agency shall authorize, monitor, and control all methods of remote access to the information system.	1	Agency	Both	Both
279			"	The agency shall employ automated mechanisms to facilitate the monitoring and control of remote access methods.	1	Agency	Both	Both
280			"	The agency shall control all remote accesses through managed access control points.	1	Agency	Both	Both
281			"	The agency may permit remote access for privileged functions only for compelling operational needs but shall document the technical and administrative process for enabling remote access for privileged functions in the security plan for the system.	1	Agency	Both	Both
			"	Virtual escorting of privileged functions is permitted only when all the following conditions are met:				
282	5.5.6	5.5.6	"	1. The session shall be monitored at all times by an authorized escort.	1	Agency	Both	Both
283			"	2. The escort shall be familiar with the system/area in which the work is being performed.	1	Agency	Both	Both
284			"	3. The escort shall have the ability to end the session at any time.	1	Agency	Both	Both
285			"	4. The remote administrative personnel connection shall be via an encrypted (FIPS 140-2 certified) path.	1	Agency	Both	Both
286			"	5. The remote administrative personnel shall be identified prior to access and authenticated prior to or during the session. This authentication may be accomplished prior to the session via an Advanced Authentication (AA) solution or during the session via active teleconference with the escort throughout the session.	1	Agency	Both	Both
287			Personally Owned Information Systems	A personally owned information system shall not be authorized to access, process, store or transmit C.J.I unless the agency has established and documented the specific terms and conditions for personally owned information system usage.	1	Agency	Both	Both
288	5.5.6.1	5.5.6.1	"	When personally owned mobile devices (i.e. bring your own device [BYOD]) are authorized, they shall be controlled in accordance with the requirements in Policy Area 13: Mobile Devices.	1	Agency	Both	Both
289	5.5.6.2	5.5.6.2	Publicly Accessible Computers	Publicly accessible computers shall not be used to access, process, store or transmit C.J.I. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.	1	Agency	Both	Both

	Ver 5.8 Location and New Requirement	Ver 5.9 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy Area 6 - Identification and Authentication								
290	5.6	5.6	Policy Area 6: Identification and Authentication	The agency shall identify information system users and processes acting on behalf of users and authenticate the identities of those users or processes as a prerequisite to allowing access to agency information systems or services.	1	Agency	Both	Both
291			Identification Policy and Procedures	Each person who is authorized to store, process, and/or transmit CJI shall be uniquely identified.	1	Agency	Both	Both
292			"	A unique identification shall also be required for all persons who administer and maintain the system(s) that access CJI or networks leveraged for CJI transit.	1	Agency	Both	Both
293	5.6.1	5.6.1	"	Agencies shall require users to identify themselves uniquely before the user is allowed to perform any actions on the system.	1	Agency	Both	Both
294			"	Agencies shall ensure that all user IDs belong to currently authorized users.	1	Agency	Both	Both
295			"	Identification data shall be kept current by adding new users and disabling and/or deleting former users.	1	Agency	Both	Both
296			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.	1	Agency	Agency	Agency
297	5.6.1.1	5.6.1.1	"	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.	1	Agency	Agency	Agency
298			"	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.	1	Agency	Agency	Agency
299			"	Agencies assigned a P (limited access) ORI shall not use the full access ORI of another agency to conduct an inquiry transaction.	1	Agency	Agency	Agency
300			Authentication Policy and Procedures	Each individual's identity shall be authenticated at either the local agency, CSA, SIB or Channeler level.	1	Agency	Agency	Agency
301			"	The authentication strategy shall be part of the agency's audit for policy compliance.	2	Agency	Agency	Agency
302	5.6.2	5.6.2	"	The FBI CJIS Division shall identify and authenticate all individuals who establish direct web-based interactive sessions with FBI CJIS Services.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
303			"	The FBI CJIS Division shall authenticate the ORI of all message-based sessions between the FBI CJIS Division and its customer agencies but will not further authenticate the user nor capture the unique identifier for the originating operator because this function is performed at the local agency, CSA, SIB or Channeler level.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
304	5.6.2.1	5.6.2.1	Standard Authenticators	Users shall not be allowed to use the same password or PIN in the same logon sequence.	1	Agency	Both	Both
305	5.6.2.1.1	5.6.2.1.1	Password	When agencies use a password as an authenticator for an individual's unique ID, they shall use the basic password standards in 5.6.2.1.1. OR follow the advanced passwords standards in 5.6.2.1.1.2.	1	Agency	Both	Both
306	5.6.2.1.1.1	5.6.2.1.1.1	Basic Password Standards	When agencies elect to follow the basic password standards, passwords shall :	1	Agency	Both	Both
307			"	1. Be a minimum length of eight (8) characters on all systems.	1	Agency	Both	Both
308			"	2. Not be a dictionary word or proper name.	1	Agency	Both	Both
309			"	3. Not be the same as the Userid.	1	Agency	Both	Both
310	5.6.2.1.1.1	5.6.2.1.1.1	"	4. Expire within a maximum of 90 calendar days.	1	Agency	Both	Both
311			"	5. Not be identical to the previous ten (10) passwords.	2	Agency	Both	Both
312			"	6. Not be transmitted in the clear outside the secure location.	1	Agency	Both	Both

	Ver 5.8 Location and New Requirement	Ver 5.9 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
313	5.6.2.1.1.1	5.6.2.1.1.1	Basic Password Standards (continued)	7. Not be displayed when entered.	1	Agency	Both	Both
			Advanced Password Standards	When agencies elect to follow the advanced password standards, follow the guidance below:				
314			"	1. Passwords shall be a minimum of twenty (20) characters in length with no additional complexity requirements imposed (e.g., ASCII characters, emojis, all keyboard characters, and spaces will be acceptable).	1	Agency	Both	Both
315			"	2. Password Verifiers shall not permit the use of a stored "hint" for forgotten passwords and/or prompt subscribers to use specific types of information (e.g., "What was the name of your first pet?") when choosing a password.	1	Agency	Both	Both
316			"	3. Verifiers shall maintain a list of "banned passwords" that contains values known to be commonly-used, expected, or compromised.	1	Agency	Both	Both
317			"	4. When processing requests to establish and change passwords, Verifiers shall compare the prospective passwords against the "banned passwords" list.	1	Agency	Both	Both
			"	5. If the chosen password is found to be part of a "banned passwords" list, the Verifier shall :				
318			"	a. Advise the subscriber that they need to select a different password.	1	Agency	Both	Both
319			"	b. Provide the reason for rejection, and	1	Agency	Both	Both
320		5.6.2.1.1.2	"	c. Require the subscriber to choose a different password.	1	Agency	Both	Both
321			"	6. Verifiers shall limit the number of failed authentication attempts that can be made as described in Section 5.5.3 Unsuccessful Login Attempts.	1	Agency	Both	Both
322			"	7. Verifiers shall force a password change if there is evidence of authenticator compromise or every 365 days from the last password change.	1	Agency	Both	Both
323			"	8. Verifiers shall use approved encryption and an authenticated protected channel when requesting passwords to protect against eavesdropping and Man-in-the-Middle (MitM) attacks.	1	Agency	Both	Both
324			"	9. Verifiers shall store passwords in a manner that is resistant to offline attacks by salting and hashing the password using a one-way key derivation function when stored.	1	Agency	Both	Both
325			"	a. The salt shall be at least 32 bits in length.	1	Agency	Both	Both
326			"	b. The salt shall be chosen arbitrarily so as to minimize salt value collisions among stored hashes.	1	Agency	Both	Both
327			"	10. For each subscriber, Verifiers shall protect stored salt and resulting hash values using a password or PIN.	1	Agency	Both	Both
328				When agencies implement the use of a PIN as a standard authenticator, the PIN attributes shall follow the guidance in section 5.6.2.1.1 (password). When agencies utilize a PIN in conjunction with a certificate or a token (e.g. key fob with rolling numbers) for the purpose of advanced authentication, agencies shall follow the PIN attributes described below.	1	Agency	Both	Both
329			Personal Identification Number (PIN)	1. Be a minimum length of six (6) digits.	1	Agency	Both	Both
330		5.6.2.1.2		2. Have no repeating digits (i.e., 112233).	1	Agency	Both	Both
331				3. Have no sequential patterns (i.e., 123456).	1	Agency	Both	Both
332				4. Not be the same as the Userid.	1	Agency	Both	Both
333				5. Expire within a maximum of 365 days.	1	Agency	Both	Both
334				6. Not be identical to the previous three (3) PINs.	1	Agency	Both	Both
335				7. Not be transmitted in the clear outside the secure location.	1	Agency	Both	Both
336				8. Not be displayed when entered.	1	Agency	Both	Both

	Ver 5.8 Location and New Requirement	Ver 5.9 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
			One-time Passwords (OTP)	When agencies implement the use of an OTP as authenticator, the OTP shall meet the requirements described below. 1. Be a minimum of six (6) randomly generated characters. 2. Be valid for a single session. 3. If not used, expire within a maximum of five (5) minutes after issuance.	1	Agency	Both	Both
337	5.6.2.1.3	5.6.2.1.3	"		1	Agency	Both	Both
338			"		1	Agency	Both	Both
339			"		1	Agency	Both	Both
			Advanced Authentication	When user-based certificates are used for authentication purposes, they shall: 1. Be specific to an individual user and not to a particular device. 2. Prohibit multiple users from utilizing the same certificate. 3. Require the user to "activate" that certificate for each user in some manner (e.g., passphrase or user-specific PIN)	1	Agency	Both	Both
340			"		1	Agency	Both	Both
341			"		1	Agency	Both	Both
342	5.6.2.2	5.6.2.2	"		1	Agency	Both	Both
343			Advanced Authentication Policy and Rationale	AA shall not be required for users requesting access to CJI from within the perimeter of a physically secure location (Section 5.9), when the technical security controls have been met (Sections 5.5 and 5.10), or... ... or when the user has no ability to conduct transactional activities on state and national repositories, applications, or services (i.e. indirect access). Conversely, if the technical security controls have not been met, AA shall be required even if the request for CJI originates from within a physically secure location.	1	Agency	Both	Both
344			"		1	Agency	Both	Both
345	5.6.2.2.1	5.6.2.2.1	"		1	Agency	Both	Both
346			"	The two authentication factors shall be unique (i.e. password/token or biometric/password but not password/password or token/token). EXCEPTION: AA shall be required when the requested service has built AA into its processes and requires a user to provide AA before granting access. The agency shall establish identifier and authenticator management processes.	1	Agency	Both	Both
347			"		1	Agency	Both	Both
348	5.6.3	5.6.3	Identifier and Authenticator Management	In order to manage user identifiers, agencies shall: 1. Uniquely identify each user. 2. Verify the identity of each user. 3. Receive authorization to issue a user identifier from an appropriate agency official. 4. Issue the user identifier to the intended party. 5. Disable the user identifier after a specified period of inactivity. 6. Archive user identifiers.	1	Agency	Both	Both
349			Identifier Management		1	Agency	Both	Both
350			"		1	Agency	Both	Both
351	5.6.3.1	5.6.3.1	"		1	Agency	Both	Both
352			"		1	Agency	Both	Both
353			"		1	Agency	Both	Both
354			"		1	Agency	Both	Both
			Authenticator Management	In order to manage information system authenticators, agencies shall: 1. Define initial authenticator content. 2. Establish administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators. 3. Change default authenticators upon information system installation. 4. Change/refresh authenticators periodically. Users shall take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and immediately reporting lost or compromised authenticators. Assertion mechanisms used to communicate the results of a remote authentication to other parties shall be: 1. Digitally signed by a trusted entity (e.g., the identity provider). 2. Obtained directly from a trusted entity (e.g. trusted broker) using a protocol where the trusted entity authenticates to the relying party using a secure protocol (e.g. transport layer security [TLS]) that cryptographically authenticates the verifier and protects the assertion.	1	Agency	Both	Both
355			"		1	Agency	Both	Both
356			"		1	Agency	Both	Both
357	5.6.3.2	5.6.3.2	"		1	Agency	Both	Both
358			"		1	Agency	Both	Both
359			"		1	Agency	Both	Both
			Assertions					
360			"		1	Agency	Both	Both
361	5.6.4	5.6.4	"		1	Agency	Both	Both

	Ver 5.8 Location and New Requirement	Ver 5.9 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
362	5.6.4	5.6.4	Assertions (continued)	Assertions generated by a verifier shall expire after 12 hours and...	1	Agency	Both	Both
363			"	...and shall not be accepted thereafter by the relying party.	1	Agency	Both	Both

	Ver 5.8 Location and New Requirement	Ver 5.9 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
C.JIS Security Policy Area 7 - Configuration Management								
364	5.7.1.1	5.7.1.1	Least Functionality	The agency shall configure the application, service, or information system to provide only essential capabilities and....	2	Agency	Both	Both
365			"	...and shall specifically prohibit and/or restrict the use of specified functions, ports, protocols, and/or services.	1	Agency	Both	Both
366			Network Diagram	The agency shall ensure that a complete topological drawing depicting the interconnectivity of the agency network, to criminal justice information, systems and services is maintained in a current status.	1	Agency	Both	Both
			"	The network topological drawing shall include the following:				
367			"	1. All communications paths, circuits, and other components used for the interconnection, beginning with the agency-owned system(s) and traversing through all interconnected systems to the agency end-point.	1	Agency	Both	Both
368	5.7.1.2	5.7.1.2	"	2. The logical location of all components (e.g., firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations). Individual workstations (clients) do not have to be shown; the number of clients is sufficient.	1	Agency	Both	Both
369			"	3. "For Official Use Only" (FOUO) markings.	1	Agency	Both	Both
370			"	4. The agency name and date (day, month, and year) drawing was created or updated.	1	Agency	Both	Both
371	5.7.2	5.7.2	Security of Configuration Documentation	Agencies shall protect the system documentation from unauthorized access consistent with the provisions described in section 5.5 Access Control.	2	Agency	Both	Both

	Ver 5.8 Location and New Requirement	Ver 5.9 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy Area 8 - Media Protection								
372	5.8	5.8	Policy Area 8: Media Protection	Media protection policy and procedures shall be documented and implemented to ensure that access to electronic and physical media in all forms is restricted to authorized individuals.	2	Agency	Agency	Agency
373			"	Procedures shall be defined for securely handling, transporting and storing media.	2	Agency	Agency	Agency
374			Media Storage and Access	The agency shall securely store electronic and physical media within physically secure locations or controlled areas.	1	Both	Both	Both
375	5.8.1	5.8.1	"	The agency shall restrict access to electronic and physical media to authorized individuals.	1	Both	Both	Both
376			"	If physical and personnel restrictions are not feasible then the data shall be encrypted per section 5.10.1.2.	1	Both	Both	Both
377	5.8.2	5.8.2	Media Transport	The agency shall protect and control electronic and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel.	1	Agency	Agency	Agency
378			Electronic Media in Transit	Controls shall be in place to protect digital media containing CJJ while in transport (physically moved from one location to another) to help prevent compromise of the data.	1	Agency	Agency	Agency
379	5.8.2.1	5.8.2.1	"	Encryption, as defined in section 5.10.1.2 of this policy, is the optimal control during transport; however, if encryption of the data isn't possible then each agency shall institute physical controls to ensure the security of the data.	1	Agency	Both	Both
380	5.8.2.2	5.8.2.2	Physical Media in Transit	Physical media shall be protected at the same level as the information would be protected in electronic form.	1	Agency	Agency	Agency
381			Electronic Media Sanitization and Disposal	The agency shall sanitize, that is, overwrite at least three times or degauss electronic media prior to disposal or release for reuse by unauthorized individuals.	1	Agency	Both	Both
382	5.8.3	5.8.3	"	Inoperable electronic media shall be destroyed (cut up, shredded, etc.).	1	Agency	Agency	Agency
383			"	The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media.	2	Agency	Agency	Agency
384			"	Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.	1	Agency	Agency	Agency
385			Disposal of Physical Media	Physical media shall be securely disposed of when no longer required, using formal procedures.	1	Agency	Agency	Agency
386	5.8.4	5.8.4	"	Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information compromise by unauthorized individuals.	2	Agency	Agency	Agency
387			"	Physical media shall be destroyed by shredding or incineration.	1	Agency	Agency	Agency
388			"	Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel.	1	Agency	Agency	Agency

	Ver 5.8 Location and New Requirement	Ver 5.9 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy Area 9 - Physical Protection								
389	5.9	5.9	Policy Area 9: Physical Protection	Physical protection policy and procedures shall be documented and implemented to ensure CJJ and information system hardware, software, and media are physically protected through access control measures.	2	Both	Both	Both
390	5.9.1.1	5.9.1.1	Security Perimeter	The perimeter of physically secure location shall be prominently posted and separated from non-secure locations by physical controls.	1	Both	Both	Both
391			"	Security perimeters shall be defined, controlled and secured in a manner acceptable to the CSA or SIB.	1	Both	Both	Both
392	5.9.1.2	5.9.1.2	Physical Access Authorizations	The agency shall develop and keep current a list of personnel with authorized access to the physically secure location (except for those areas within the permanent facility officially designated as publicly accessible) or...	1	Both	Both	Both
393			"	...or shall issue credentials to authorized personnel.	1	Both	Both	Both
394	5.9.1.3	5.9.1.3	Physical Access Control	The agency shall control all physical access points (except for those areas within the facility officially designated as publicly accessible) and...	1	Both	Both	Both
395			"	...and shall verify individual access authorizations before granting access.	1	Both	Both	Both
396	5.9.1.4	5.9.1.4	Access Control for Transmission Medium	The agency shall control physical access to information system distribution and transmission lines within the physically secure location.	1	Both	Both	Both
397	5.9.1.5	5.9.1.5	Access Control for Display Medium	The agency shall control physical access to information system devices that display CJJ and...	1	Both	Both	Both
398			"	...and shall position information system devices in such a way as to prevent unauthorized individuals from accessing and viewing CJJ.	1	Both	Both	Both
399	5.9.1.6	5.9.1.6	Monitoring Physical Access	The agency shall monitor physical access to the information system to detect and respond to physical security incidents.	1	Both	Both	Both
400	5.9.1.7	5.9.1.7	Visitor Control	The agency shall control physical access by authenticating visitors before authorizing escorted access to the physically secure location (except for those areas designated as publicly accessible).	1	Both	Both	Both
401			"	The agency shall escort visitors at all times and monitor visitor activity.	1	Both	Both	Both
402	5.9.1.8	5.9.1.8	Delivery and Removal	The agency shall authorize and control information system-related items entering and exiting the physically secure location.	1	Both	Both	Both
403			Controlled Area	If an agency cannot meet all of the controls required for establishing a physically secure location, but has an operational need to access or store CJJ, the agency shall designate an area, a room, or a storage container, as a "controlled area" for the purpose of day-to-day CJJ access or storage.	1	Both	Both	Both
			"	The agency shall , at a minimum:				
404	5.9.2	5.9.2	"	1. Limit access to the controlled area during CJJ processing times to only those personnel authorized by the agency to access or view CJJ.	1	Both	Both	Both
405			"	2. Lock the area, room, or storage container when unattended.	1	Both	Both	Both
406			"	3. Position information system devices and documents containing CJJ in such a way as to prevent unauthorized individuals from access and view.	1	Both	Both	Both
407			"	4. Follow the encryption requirements found in section 5.10.1.1.2 for electronic storage (i.e. data "at rest") of CJJ.	1	Both	Both	Both

	Ver 5.8 Location and New Requirement	Ver 5.9 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
C.JIS Security Policy Area 10 - Systems and Communications Protection and Information Integrity								
408	5.10.1	5.10.1	Information Flow Enforcement	The network infrastructure shall control the flow of information between interconnected systems. The agency shall:	1	Both	Service Provider	Service Provider
409			Boundary Protection	1. Control access to networks processing CJI.	1	Both	Service Provider	Service Provider
410			"	2. Monitor and control communications at the external boundary of the information system and at key internal boundaries within the system.	1	Both	Service Provider	Service Provider
411			"	3. Ensure any connections to the Internet, other external networks, or information systems occur through controlled interfaces (e.g. proxies, gateways, routers, firewalls, encrypted tunnels). See Section 5.10.4.4 for guidance on personal firewalls.	1	Both	Service Provider	Service Provider
412	5.10.1.1	5.10.1.1	"	4. Employ tools and techniques to monitor network events, detect attacks, and provide identification of unauthorized use.	1	Both	Service Provider	Service Provider
413			"	5. Ensure the operational failure of the boundary protection mechanisms do not result in any unauthorized release of information outside of the information system boundary (i.e. the device "fails closed" vs. "fails open").	1	Both	Service Provider	Service Provider
414			"	6. Allocate publicly accessible information system components (e.g. public Web servers) to separate sub networks with separate, network interfaces. Publicly accessible information systems residing on a virtual host shall follow the guidance in section 5.10.3.2 to achieve separation.	1	Both	Service Provider	Service Provider
415			Encryption for CJI in Transit	When CJI is transmitted outside the boundary of the physically secure location, the data shall be immediately protected via encryption.	1	Both	Service Provider	Service Provider
416			"	When encryption is employed, the cryptographic module used shall be FIPS 140-2 certified and ...	1	Both	Service Provider	Service Provider
417			"	... and use a symmetric cipher key strength of at least 128 bit strength to protect CJI.	1	Both	Service Provider	Service Provider
418			"	2. Encryption shall not be required if the transmission medium meets all of the following requirements:				
419	5.10.1.2.1	5.10.1.2.1	"	a. The agency owns, operates, manages, or protects the medium.	1	Agency	Agency	Agency
420			"	b. Medium terminates within physically secure locations at both ends with no interconnections between.	1	Agency	Agency	Agency
421			"	c. Physical access to the medium is controlled by the agency using the requirements in Section 5.9.1 and 5.1.2.	1	Agency	Agency	Agency
422			"	d. Protection includes safeguards (e.g. acoustic, electric, electromagnetic, and physical) and if feasible countermeasures (e.g. alarms, notifications) to permit its use for the transmission of unencrypted information through an area of lesser classification or control.	1	Agency	Agency	Agency
423			"	e. With approval of the CSO.	1	Agency	Agency	Agency
424			Encryption for CJI at Rest	When CJI is at rest (i.e. stored electronically) outside the boundary of the physically secure location, the data shall be protected via encryption.	1	Both	Service Provider	Service Provider
425	5.10.1.2.2	5.10.1.2.2	"	When encryption is employed, agencies shall either encrypt CJI in accordance with the standard in Section 5.10.1.2.1 above, or ...	1	Both	Service Provider	Service Provider
426			"	... or use a symmetric cipher that is FIPS 197 certified (AES) and at least 256 bit strength.	1	Both	Service Provider	Service Provider
427			"	1. When agencies implement encryption on CJI at rest, the passphrase to unlock the cipher shall meet the following requirements: a. Be at least 10 characters b. Not be a dictionary word	1	Both	Service Provider	Service Provider

	Ver 5.8 Location and New Requirement	Ver 5.9 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
428			Encryption for CJJ at Rest (continued)	c. Include at least one (1) upper case letter, one (1) lower case letter, one (1) number, and one (1) special character. d. Be changed when previously authorized personnel no longer require access	1	Both	Service Provider	Service Provider
429			"		1	Both	Service Provider	Service Provider
430	5.10.1.2.2	5.10.1.2.2	"	2. Multiple files maintained in the same unencrypted folder shall have separate and distinct passphrases.	1	Both	Service Provider	Service Provider
431			"	2. All audit requirements found in Section 5.4.1 Auditable Events and Content (Information Systems) shall be applied.	1	Both	Service Provider	Service Provider
432			Public Key Infrastructure (PKI) Technology	For agencies using public key infrastructure (PKI) technology, the agency shall develop and implement a certificate policy and certification practice statement for the issuance of public key certificates used in the information system.	1	Both	Service Provider	Service Provider
			"	Registration to receive a public key certificate shall :				
433	5.10.1.2.3	5.10.1.2.3	"	1. Include authorization by a supervisor or a responsible official.	1	Both	Service Provider	Service Provider
434			"	2. Be accomplished by a secure process that verifies the identity of the certificate holder.	1	Both	Service Provider	Service Provider
435			"	3. Ensure the certificate is issued to the intended party.	1	Both	Service Provider	Service Provider
			Intrusion Detection Tools and Techniques	Agencies shall :				
436			"	1. Implement network-based and/or host-based intrusion detection or prevention tools.	1	Both	Service Provider	Service Provider
437			"	2. Maintain current intrusion detection or prevention signatures.	1	Both	Service Provider	Service Provider
438	5.10.1.3	5.10.1.3	"	3. Monitor inbound and outbound communications for unusual or unauthorized activities.	1	Both	Service Provider	Service Provider
439			"	4. Send individual intrusion detection logs to a central logging facility where correlation and analysis will be accomplished as a system wide intrusion detection effort.	1	Both	Service Provider	Service Provider
440			"	5. Review intrusion detection or prevention logs weekly or implement automated event notification.	1	Both	Service Provider	Service Provider
441			"	6. Employ automated tools to support near-real-time analysis of events in support of detecting system-level attacks.	1	Both	Service Provider	Service Provider
			Voice over Internet Protocol	In addition to the security controls described in this document, the following additional controls shall be implemented when an agency deploys VoIP within a network that contains unencrypted CJJ:				
442	5.10.1.4	5.10.1.4	"	1. Establish usage restrictions and implementation guidance for VoIP technologies.	1	Both	Service Provider	Service Provider
443			"	2. Document, monitor and control the use of VoIP within the agency.	1	Both	Service Provider	Service Provider
444			"	3. Utilize Virtual Local Area Network (VLAN) technology to segment VoIP traffic from data traffic.	1	Both	Service Provider	Service Provider
445			Cloud Computing	The storage of CJJ, regardless of encryption status, shall only be permitted in cloud environments (e.g. government or third-party/commercial datacenters, etc.) which reside within the physical boundaries of APB-member country (i.e. U.S., U.S. territories, Indian Tribes, and Canada) and legal authority of an APB-member agency (i.e. U.S. – federal/state/territory, Indian Tribe, or the Royal Canadian Mounted Police (RCMP)).	1	Service Provider	Service Provider	Service Provider
446	5.10.1.5	5.10.1.5	"	Metadata derived from unencrypted CJJ shall be protected in the same manner as CJJ and...	1	Service Provider	Service Provider	Service Provider
447			"	...and shall not be used for any advertising or other commercial purposes by any cloud service provider or other associated entity.	1	Service Provider	Service Provider	Service Provider

	Ver 5.8 Location and New Requirement	Ver 5.9 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
448	5.10.2	5.10.2	Facsimile Transmission of CJI	CJI transmitted external to a physically secure location using a facsimile server, application or service which implements email-like technology, shall meet the encryption requirements for CJI in transit as defined in Section 5.10.	1	Both	Service Provider	Service Provider
449	5.10.3.1	5.10.3.1	Partitioning	The application, service, or information system shall separate user functionality (including user interface services) from information system management functionality.	2	Both	Service Provider	Service Provider
450			"	The application, service, or information system shall physically or logically separate user interface services (e.g. public Web pages) from information storage and management services (e.g. database management).	1	Both	Service Provider	Service Provider
			Virtualization	In addition to the security controls described in this policy, the following additional controls shall be implemented in a virtual environment:				
451			"	1. Isolate the host from the virtual machine. In other words, virtual machine users cannot access host files, firmware, etc.	1	Both	Service Provider	Service Provider
452			"	2. Maintain audit logs for all virtual machines and hosts and store the logs outside the hosts' virtual environment.	2	Both	Service Provider	Service Provider
453			"	3. Virtual Machines that are Internet facing (web servers, portal servers, etc.) shall be physically separate from Virtual Machines that process CJI internally or be separated by a virtual firewall.	1	Both	Service Provider	Service Provider
454	5.10.3.2	5.10.3.2	"	4. Drivers that serve critical functions shall be stored within the specific VM they service. In other words, do not store these drivers within the hypervisor, or host operating system, for sharing. Each VM is to be treated as an independent system - secured as independently as possible.	1	Both	Service Provider	Service Provider
			"	The following additional technical security controls shall be applied in virtual environments where CJI is commingled with non-CJI:				
455			"	1. Encrypt CJI when stored in a virtualized environment where CJI is commingled with non-CJI or segregate and store unencrypted CJI within its own secure VM.	1	Both	Service Provider	Service Provider
456			"	2. Encrypt network traffic within the virtual environment.	1	Both	Service Provider	Service Provider
457			Patch Management	The agency shall identify applications, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws.	1	Both	Service Provider	Service Provider
458	5.10.4.1	5.10.4.1	"	The agency (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor) shall develop and implement a local policy that ensures prompt installation of newly released security relevant patches, service packs and hot fixes.	1	Both	Service Provider	Service Provider
459			"	Patch requirements discovered during security assessments, continuous monitoring or incident response activities shall also be addressed expeditiously.	1	Both	Service Provider	Service Provider
460			Malicious Code Protection	The agency shall implement malicious code protection that includes automatic updates for all systems with Internet access.	1	Both	Service Provider	Service Provider
461			"	Agencies with systems not connected to the Internet shall implement local procedures to ensure malicious code protection is kept current (i.e. most recent update available).	1	Both	Service Provider	Service Provider
462	5.10.4.2	5.10.4.2	"	The agency shall employ virus protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses) at critical points throughout the network and on all workstations, servers and mobile computing devices on the network.	1	Both	Service Provider	Service Provider
463			"	The agency shall ensure malicious code protection is enabled on all of the aforementioned critical points and information systems and resident scanning is employed.	1	Both	Service Provider	Service Provider

	Ver 5.8 Location and New Requirement	Ver 5.9 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
464			Spam and Spyware Protection	The agency shall implement spam and spyware protection.	2	Both	Service Provider	Service Provider
465			"	The agency shall : 1. Employ spam protection mechanisms at critical information system entry points (e.g. firewalls, electronic mail servers, remote-access servers).	2	Both	Service Provider	Service Provider
466	5.10.4.3	5.10.4.3	"	2. Employ spyware protection at workstations, servers and mobile computing devices on the network. 3. Use the spam and spyware protection mechanisms to detect and take appropriate action on unsolicited messages and spyware/adware, respectively, transported by electronic mail, electronic mail attachments, Internet accesses, removable media (e.g. diskettes or compact disks) or other removable media as defined in this policy document.	2	Both	Service Provider	Service Provider
467			"	The agency shall : 1. Receive information system security alerts/advisories on a regular basis.	2	Both	Service Provider	Service Provider
468			Security Alerts and Advisories	2. Issue alerts/advisories to appropriate personnel.	2	Both	Service Provider	Service Provider
469			"	3. Document the types of actions to be taken in response to security alerts/advisories.	2	Both	Service Provider	Service Provider
470	5.10.4.4	5.10.4.4	"	4. Take appropriate actions in response.	2	Both	Service Provider	Service Provider
471			"	5. Employ automated mechanisms to make security alert and advisory information available throughout the agency as appropriate.	2	Both	Service Provider	Service Provider
472			"	The agency shall restrict the information input to any connection to FBI CJIS services to authorized personnel only.	2	Both	Service Provider	Service Provider
473	5.10.4.5	5.10.4.5	Information Input Restrictions		1	Agency	Agency	Agency

	Ver 5.8 Location and New Requirement	Ver 5.9 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy Area 11 - Formal Audits								
474			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.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
475	5.11.1.1	5.11.1.1	"	This audit shall include a sample of CJsAs and, in coordination with the SIB, the NCJAs.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
476			"	The FBI CJIS Division shall also have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
477	5.11.1.2	5.11.1.2	Triennial Security Audits by the FBI CJIS Division	This audit shall include a sample of CJsAs and NCJAs.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
			Audits by the CSA	Each CSA shall:				
478			"	1. At a minimum, triennially audit all CJsAs and NCJAs which have direct access to the state system in order to ensure compliance with applicable statutes, regulations and policies.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
479			"	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.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
480	5.11.2	5.11.2	"	3. Have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
481			"	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.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
482			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.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
483			"	The inspection team shall be appointed by the APB and...	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
484	5.11.3	5.11.3	"	...and shall include at least one representative of the CJIS Division.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
485			"	All results of the inquiry and audit shall be reported to the APB with appropriate recommendations.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO

	Ver 5.8 Location and New Requirement	Ver 5.9 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJS Security Policy Area 12 - Personnel Security								
486			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).	1	Agency	Agency	Agency
487			"	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 CHR1 IQ/FQ/IAQ query using purpose code C, E, or J depending on the circumstances.	1	Agency	Agency	Agency
488			"	When appropriate, the screening shall be consistent with a. 5 CFR 731.106; and/or b. Office of Personnel Management policy, regulations, and guidance; and/or c. agency policy, regulations, and guidance.	1	Agency	Agency	Agency
489			"	2. All requests for access shall be made as specified by the CSO.	1	Agency	Agency	Agency
490			"	All CSO designees shall be from an authorized criminal justice agency.	1	Agency	Agency	Agency
491			"	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.	1	Agency	Agency	Agency
492	5.12.1	5.12.1	"	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.	1	Agency	Agency	Agency
493			"	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.	1	Agency	Agency	Agency
494			"	c. (cont) The CGA shall in turn notify the contractor's security officer.	1	Agency	Agency	Agency
495			"	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.	1	Agency	Agency	Agency
496			"	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.	1	Agency	Agency	Agency
497			"	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...	1	Agency	Agency	Agency
498			"	...and the person's appointing authority shall be notified in writing of the access denial.	1	Agency	Agency	Agency
499			"	7. The granting agency shall maintain a list of personnel who have been authorized unescorted access to unencrypted CJI and...	1	Agency	Agency	Agency
500			"	...and shall , upon request, provide a current copy of the access list to the CSO.	1	Agency	Agency	Agency
501	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.	1	Both	Both	Both
502	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.	1	Both	Both	Both
503	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.	1	Both	Both	Both
504	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.	1	Both	Both	Both
505	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.	2	Both	Both	Both

	Ver 5.8 Location and New Requirement	Ver 5.9 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy Area 13 - Mobile Devices								
			Mobile Devices	The agency shall:				
506	5.13	5.13	"	(i) establish usage restrictions and implementation guidance for mobile devices;	1	Agency	Agency	Agency
507			"	(ii) authorize, monitor, control wireless access to the information system.	1	Agency	Agency	Agency
508			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.	1	Agency	Agency	Agency
509			"	Agencies shall implement the following controls for all agency-managed wireless access points with access to an agency's network that processes unencrypted CJI:	1	Agency	Agency	Agency
			"	Agencies shall implement the following controls for all agency-managed wireless access points:				
510			"	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.	1	Agency	Agency	Agency
511			"	2. Maintain a complete inventory of all Access Points (APs) and 802.11 wireless devices.	1	Agency	Agency	Agency
512			"	3. Place APs in secured areas to prevent unauthorized physical access and user manipulation.	1	Agency	Agency	Agency
513			"	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.	1	Agency	Agency	Agency
514			"	5. Enable user authentication and encryption mechanisms for the management interface of the AP.	1	Agency	Agency	Agency
515			"	6. Ensure that all APs have strong administrative passwords and ensure that all passwords are changed in accordance with section 5.6.3.1.	1	Agency	Agency	Agency
516	5.13.1.1	5.13.1.1	"	7. Ensure the reset function on APs is used only when needed and is only invoked by authorized personnel. Restore the APs to the latest security settings, when the reset functions are used, to ensure the factory default settings are not utilized.	1	Agency	Agency	Agency
517			"	8. Change the default service set identifier (SSID) in the APs.	1	Agency	Agency	Agency
518			"	Disable the broadcast SSID feature so that the client SSID must match that of the AP.	1	Agency	Agency	Agency
519			"	Validate that the SSID character string does not contain any agency identifiable information (division, department, street, etc.) or services.	1	Agency	Agency	Agency
520			"	9. Enable all security features of the wireless product, including the cryptographic authentication, firewall, and other privacy features.	1	Agency	Agency	Agency
521			"	10. Ensure that encryption key sizes are at least 128-bits and...	1	Agency	Agency	Agency
522			"	...and the default shared keys are replaced by unique keys.	1	Agency	Agency	Agency
523			"	11. Ensure that the ad hoc mode has been disabled.	1	Agency	Agency	Agency
524			"	12. Disable all nonessential management protocols on the APs. Disable non-FIPS compliant secure access to the management interface.	1	Agency	Agency	Agency
525			"	13. Ensure all management access and authentication occurs via FIPS compliant secure protocols (e.g. SFTP, HTTPS, SNMP over TLS, etc.). Disable non-FIPS compliant secure access to the management interface.	1	Agency	Agency	Agency
526			"	14. Enable logging (if supported) and...	1	Agency	Agency	Agency
527			"	...and review the logs on a recurring basis per local policy.	1	Agency	Agency	Agency
528			"	At a minimum logs shall be reviewed monthly.	1	Agency	Agency	Agency

	Ver 5.8 Location and New Requirement	Ver 5.9 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
529	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.	1	Agency	Agency	Agency
530			"	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.	1	Agency	Agency	Agency
531	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.	1	Agency	Agency	Agency
532	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.	2	Agency	Agency	Agency
			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:				
533			"	1. Enable encryption on the hotspot	1	Agency	Agency	Agency
534			"	2. Change the hotspot's default SSID	1	Agency	Agency	Agency
535	5.13.1.4	5.13.1.4	"	a. Ensure the hotspot SSID does not identify the device make/model or agency ownership	1	Agency	Agency	Agency
536			"	3. Create a wireless network password (Pre-shared key)	1	Agency	Agency	Agency
537			"	4. Enable the hotspot's port filtering/blocking features if present	1	Agency	Agency	Agency
538			"	5. Only allow connections from agency controlled devices	1	Agency	Agency	Agency
539			"	OR 1. Have a MDM solution to provide the same security as identified in 1 - 5 above.	1	Agency	Agency	Agency
540			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.	1	Agency	Agency	Agency
			"	User agencies shall implement the following controls when directly accessing allowing CJI access from devices running limited feature operating system:				
541			"	1. Ensure that CJI is only transferred between CJI authorized applications and storage areas of the device.	1	Agency	Agency	Agency
542			"	2. MDM with centralized administration configured and implemented to perform at least the following controls:	1	Agency	Agency	Agency
543			"	a. Remote locking of the device	1	Agency	Agency	Agency
544	5.13.2	5.13.2	"	b. Remote wiping of the device	1	Agency	Agency	Agency
545			"	c. Setting and locking device configuration	1	Agency	Agency	Agency
546			"	d. Detection of "rooted" and "jailbroken" devices	1	Agency	Agency	Agency
547			"	e. Enforcement of folder or disk level encryption	1	Agency	Agency	Agency
548			"	f. Application of mandatory policy settings on the device	1	Agency	Agency	Agency
549			"	g. Detection of unauthorized configurations	1	Agency	Agency	Agency
550			"	h. Detection of unauthorized software or applications	1	Agency	Agency	Agency
551			"	i. Ability to determine location of agency controlled devices	1	Agency	Agency	Agency
552			"	j. Prevention of unpatched devices from accessing CJI or C/JI systems	1	Agency	Agency	Agency
553	5.13.3	5.13.3	Wireless Device Risk Mitigations	k. Automatic device wiping after a specified number of failed access attempts	1	Agency	Agency	Agency
				Organizations shall, as a minimum, ensure that wireless devices:				

	Ver 5.8 Location and New Requirement	Ver 5.9 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
554			Wireless Device Risk Mitigations (continued)	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.	1	Agency	Agency	Agency
555			"	2. Are configured for local device authentication (see Section 5.13.8.1).	1	Agency	Agency	Agency
556			"	3. Use advanced authentication or CSO approved compensating controls as per Section 5.13.7.2.1.	1	Agency	Agency	Agency
557			"	4. Encrypt all CJI resident on the device.	1	Agency	Agency	Agency
558	5.13.3	5.13.3	"	5. Erase cached information, to include authenticators (see Section 5.6.2.1) in applications, when session is terminated.	1	Agency	Agency	Agency
559			"	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.	1	Agency	Agency	Agency
560			"	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.	1	Agency	Agency	Agency
561	5.13.4.1	5.13.4.1	Patching/Updates	Agencies shall monitor mobile devices to ensure their patch and update state is current.	1	Agency	Agency	Agency
562	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.	1	Agency	Agency	Agency
563			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).	1	Agency	Agency	Agency
				At a minimum, the personal firewall shall perform the following activities:				
564	5.13.4.3	5.13.4.3	"	1. Manage program access to the internet.	1	Agency	Agency	Agency
565			"	2. Block unsolicited requests to connect to the PC.	1	Agency	Agency	Agency
566			"	3. Filter incoming traffic by IP address or protocol.	1	Agency	Agency	Agency
567			"	4. Filter incoming traffic by destination ports.	1	Agency	Agency	Agency
568			"	5. Maintain an IP traffic log.	1	Agency	Agency	Agency
569			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.	1	Agency	Agency	Agency
				Special reporting procedures for mobile devices shall apply in any of the following situations:				
570			"	1. Loss of device control. For example:	1	Agency	Agency	Agency
			"	a. Device known to be locked, minimal duration of loss				
			"	b. Device lock state unknown, minimal duration of loss				
			"	c. Device lock state unknown, extended duration of loss				
			"	d. Device known to be unlocked, more than momentary duration of loss				
571	5.13.5	5.13.5	"	2. Total loss of device	1	Agency	Agency	Agency
572			"	3. Device compromise	1	Agency	Agency	Agency
573			"	4. Device loss or compromise outside the United States	1	Agency	Agency	Agency
574	5.13.6	5.13.6	Access Control	Access control (Section 5.5 Access Control) shall be accomplished by the application that accesses CJI.	1	Agency	Agency	Agency
575			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.	1	Agency	Agency	Agency
576	5.13.7.1	5.13.7.1	"	The authenticator used shall meet the requirements in section 5.6.2.1 Standard Authenticators.	1	Agency	Agency	Agency

	Ver 5.8 Location and New Requirement	Ver 5.9 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
577	5.13.7.2	5.13.7.2	Advanced Authentication	When accessing CJI from an authorized mobile device, advanced authentication shall be used by the authorized user unless the access to CJI is indirect as described in Section 5.6.2.2.1. If access is indirect, then AA is not required.	1	Agency	Agency	Agency
578			Compensating Controls	Before CSOs consider approval of compensating controls, Mobile Device Management (MDM) shall be implemented per Section 5.13.2. The compensating controls shall :	1	Agency	Agency	Agency
579			"	1. Meet the intent of the CJIS Security Policy AA requirement	1	Agency	Agency	Agency
580			"	2. Provide a similar level of protection or security as the original AA requirement	1	Agency	Agency	Agency
581			"	3. Not rely upon the existing requirements for AA as compensating controls	1	Agency	Agency	Agency
582	5.13.7.2.1	5.13.7.2.1	"	4. Expire upon the CSO approved date or when a compliant AA solution is implemented.	1	Agency	Agency	Agency
583			"	The following minimum controls shall be implemented as a part of the CSO approved compensating controls:				
584			"	Possession and registration of an agency-issued smartphone or tablet as an indication it is the authorized user	1	Agency	Agency	Agency
585			"	Use of device certificates as per Section 5.13.7.3 Device Certificates	1	Agency	Agency	Agency
			"	Implemented CJIS Security Policy compliant standard authenticator protection on the secure location where CJI is stored	1	Agency	Agency	Agency
			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:				
586			"	1. Protected against being extracted from the device	1	Agency	Agency	Agency
587	5.13.7.3	5.13.7.3	"	2. Configured for remote wipe on demand or self-deletion based on a number of unsuccessful login or access attempts	1	Agency	Agency	Agency
588			"	3. Configured to use a secure authenticator (i.e. password, PIN) to unlock the key for use	1	Agency	Agency	Agency