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

Requirements Companion Document to the FBI CJIS Security Policy Version 5.6 06/05/2017

Recommended changes to version 5.5 of the *CJIS Security Policy* were approved by the Advisory Policy Board (APB) in 2016 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. This document has been renamed from "Requirements and Tiering Document" to the new title above.

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 will end September 30, 2017***.

The "Summary of Changes" page lists requirements that were added, deleted, or changed from the previous version and are now reflected in the current version. 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.

This document now contains additional columns describing who (CJIS/CSO, Agency, Cloud Service Provider or both the agency and service provider) is ably responsible to perform the actions necessary to ensure a particular requirement is being met. ***NOTE: The Agency will always be 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 5.6

Requirement No.	Change
314 – 316	Add new section and requirements: Section 5.6.2.1.3 One-time Passwords (OTP)
n/a	Delete previous requirement: Section 5.10.1.2
392 – 399	Create new section: Section 5.10.1.2.1 Encryption for CJI in Transit
392	Change language: Section 5.10.1.2.1
393 – 394	Relocate requirement and change language in Section 5.10.1.2.1
395 – 399	Relocate requirements: Section 5.10.1.2.1
400 – 408	Create new section: Section 5.10.1.2.2 Encryption for CJI at Rest
400	Change language: Section 5.10.1.2.2
401 – 402	Relocate requirement and change language in Section 5.10.1.2.2
403 – 408	Relocate requirements: Section 5.10.1.2.2
n/a	Delete previous requirement in Section 5.10.1.2
409 – 412	Create new section: Section 5.10.1.2.3 Public Key Infrastructure (PKI) Technology
409	Change language: Section 5.10.1.2.3

	Ver 5.5 Location and New Requirement	Ver 5.6 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	1.3	1.3	Relationship to Local Security Policy and Other Policies	The local agency may complement the CJIS Security Policy with a local policy, or the agency may develop their own stand-alone security policy; however, the CJIS Security Policy **shall** always be the minimum standard and local policy may augment, or increase the standards,…	1	Agency	Agency	Agency
2			"	...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
			"	The CSO **shall** set, maintain, and enforce the following:				
8	3.2.2(1)	3.2.2(1)	"	1. Standards for the selection, supervision, and separation of personnel who have access to CJI.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
9	3.2.2(2)	3.2.2(2)	"	2. Policy governing the operation of computers, access devices, circuits, hubs, routers, firewalls, and other components that comprise and support a telecommunications network and related CJIS systems used to process, store, or transmit CJI, guaranteeing the priority, confidentiality, integrity, and availability of service needed by the criminal justice community.	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			"	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. The CSO, or designee, **shall** ensure that a Terminal Agency Coordinator (TAC) is designated within each agency that has devices accessing 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			"	f. Approve access to FBI CJIS systems.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
16			"	g. Assume ultimate responsibility for managing the security of CJIS systems within their state and/or agency.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
17			"	h. Perform other related duties outlined by the user agreements with the FBI CJIS Division.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
			"	3. Outsourcing of Criminal Justice Functions				
18	3.2.3(3)	3.2.3(3)	"	a. Responsibility for the management of the approved security requirements **shall** remain with the CJA.	1	Agency	Agency	Agency
19			"	b. Responsibility for the management control of network security **shall** remain with the CJA.	1	Agency	Agency	Agency
20	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 5.5 Location and New Requirement	Ver 5.6 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
21	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
	3.2.7	3.2.7	"	The AC **shall**:				
22			"	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
23			"	2. Participate in related meetings and provide input and comments for system improvement.	2	Agency	Agency	Agency
24			"	3. Receive information from the CGA (e.g., system updates) and disseminate it to appropriate Contractor employees.	1	Agency	Agency	Agency
25			"	4. Maintain and update manuals applicable to the effectuation of the agreement, and provide them to the Contractor.	2	Agency	Agency	Agency
26			"	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
27			"	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
28			"	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
29			"	8. Where appropriate, ensure compliance by the Contractor with NCIC validation requirements.	1	Agency	Agency	Agency
30			"	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
31	3.2.7	3.2.7	"	10. Any other responsibility for the AC promulgated by the FBI.	1	Agency	Agency	Agency
	3.2.8	3.2.8	CJIS System Agency Information Secrurity Officer (CSA ISO)	The CSA ISO **shall**:				
32			"	1. Serve as the security point of contact (POC) to the FBI CJIS Division ISO.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
33			"	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
34			"	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
35			"	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

	Ver 5.5 Location and New Requirement	Ver 5.6 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
	3.2.9	3.2.9	Local Agency Security Officer (LASO)	Each LASO **shall**:				
36			"	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
37			"	2. Identify and document how the equipment is connected to the state system.	1	Agency	Agency	Agency
38			"	3. Ensure that personnel security screening procedures are being followed as stated in this policy.	1	Agency	Agency	Agency
39			"	4. Ensure the approved and appropriate security measures are in place and working as expected.	1	Agency	Agency	Agency
40			"	5. Support policy compliance and ensure CSA ISO is promptly informed of security incidents.	1	Agency	Agency	Agency
	3.2.10	3.2.10	FBI CJIS Division Information Security Officer (FBI CJIS ISO)	The FBI CJIS ISO **shall**:				
41			"	1. Maintain the CJIS Security Policy.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
42			"	2. Disseminate the FBI Director approved CJIS Security Policy.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
43			"	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
44			"	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
45			"	5. Assist with developing audit compliance guidelines as well as identifying and reconciling security-related issues.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
46			"	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
47	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
48	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
49				...Compact Officer who **shall** ensure that Compact provisions and rules, procedure	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
50	4.2.1	4.2.1	Proper Access, Use, and Dissemination of CHRI	The III **shall** be accessed only for an authorized purpose.	1	Agency	Agency	Agency
51			"	Further, CHRI **shall** only be used for an authorized purpose consistent with the purpose for which III was accessed.	1	Agency	Agency	Agency
52	4.2.2	4.2.2	Proper Access, Use, and Dissemination of NCIC Restricted Files Information	Proper access to, use, and dissemination of data from restricted files **shall** be consistent with the access, use, and dissemination policies concerning the III described in Title 28, Part 20, CFR, and the NCIC Operating Manual.	1	Agency	Agency	Agency
			"	The restricted files, which **shall** be protected as CHRI, are as follows:				
53			"	1. Gang File	1	Agency	Agency	Agency
54			"	2. Known or Appropriately Suspected Terrorist File	1	Agency	Agency	Agency
55			"	3. Supervised Release File	1	Agency	Agency	Agency
56			"	4. National Sex Offender Registry File	1	Agency	Agency	Agency
57			"	5. Historical Protection Order File of the NCIC	1	Agency	Agency	Agency
58			"	6. Identity Theft File	1	Agency	Agency	Agency
59			"	7. Protective Interest File	1	Agency	Agency	Agency
60			"	8. Person With Information [PWI] data in the Missing Person Files	1	Agency	Agency	Agency
61			"	9. Violent Person File	1	Agency	Agency	Agency
62			"	10. NICS Denied Transaction File	1	Agency	Agency	Agency

	Ver 5.5 Location and New Requirement	Ver 5.6 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
63	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
64			"	Agencies **shall not** disseminate restricted files information for purposes other than law enforcement.	1	Agency	Agency	Agency
65	4.2.4	4.2.4	Storage	When CHRI is stored, agencies **shall** establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of the information.	1	Agency	Agency	Agency
66			"	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
67	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
68	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
69			"	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 5.5 Location and New Requirement	Ver 5.6 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				
70	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
71	5.1.1	5.1.1	Information Exchange	Before exchanging CJI, agencies **shall** put formal agreements in place that specify security controls.	1	Agency	Agency	Agency
72			"	Information exchange agreements for agencies sharing CJI data that is sent to and/or received from the FBI CJIS **shall** specify the security controls and conditions described in this document.	1	Agency	Agency	Agency
73			"	Information exchange agreements **shall** be supported by documentation committing both parties to the terms of information exchange.	1	Agency	Agency	Agency
74			"	Law Enforcement and civil agencies **shall** have a local policy to validate a requestor of CJI as an authorized recipient before disseminating CJI.	1	Agency	Agency	Agency
75	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
76			"	Using the requirements in this policy as a starting point, the procedures **shall** apply to the handling, processing, storing, and communication of CJI.	1	Agency	Agency	Agency
77	5.1.1.2	5.1.1.2	State and Federal Agency User Agreements	Each CSA head or SIB Chief **shall** execute a signed written user agreement with the FBI CJIS Division stating their willingness to demonstrate conformity with this policy before accessing and participating in CJIS records information programs.	1	Agency	Agency	Agency
78			"	This agreement **shall** include the standards and sanctions governing utilization of CJIS systems.	1	Agency	Agency	Agency
79			"	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
80			"	All user agreements with the FBI CJIS Division **shall** be coordinated with the CSA head.	1	Agency	Agency	Agency
81	5.1.1.3	5.1.1.3	Criminal Justice Agency User Agreements	Any CJA receiving access to FBI CJI **shall** enter into a signed written agreement with the appropriate signatory authority of the CSA providing the access.	1	Agency	Agency	Agency
82			"	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:				
83			"	1. Audit.	1	Agency	Agency	Agency
84			"	2. Dissemination.	1	Agency	Agency	Agency
85			"	3. Hit confirmation.	1	Agency	Agency	Agency
86			"	4. Logging.	1	Agency	Agency	Agency
87			"	5. Quality Assurance (QA).	1	Agency	Agency	Agency
88			"	6. Screening (Pre-Employment).	1	Agency	Agency	Agency
89			"	7. Security.	1	Agency	Agency	Agency
90			"	8. Timeliness.	1	Agency	Agency	Agency
91			"	9. Training.	1	Agency	Agency	Agency
92			"	10. Use of the system.	1	Agency	Agency	Agency
93			"	11. Validation.	1	Agency	Agency	Agency
94	5.1.1.4	5.1.1.4	Inter-Agency and Management Control Agreements	A NCJA (government) designated to perform criminal justice functions for a CJA **shall** be eligible for access to the CJI.	1	Agency	Agency	Agency
95			"	Access **shall** be permitted when such designation is authorized pursuant to Executive Order, statute, regulation, or inter-agency agreement.	1	Agency	Agency	Agency

	Ver 5.5 Location and New Requirement	Ver 5.6 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
96	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
97	5.1.1.5	5.1.1.5	Private Contractor User Agreements and CJIS Security Addendum	Private contractors who perform criminal justice functions **shall** meet the same training and certification criteria required by governmental agencies performing a similar function, and…	1	Both	Both	Both
98			"	...and **shall** be subject to the same extent of audit review as are local user agencies.	1	Both	Both	Both
99			"	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
100			"	Modifications to the CJIS Security Addendum **shall** be enacted only by the FBI.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
101			"	1. Private contractors designated to perform criminal justice functions for a CJA **shall** be eligible for access to CJI.	1	Agency	Agency	Agency
102			"	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
103			"	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
104			"	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
105			"	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
106			"	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
107	5.1.1.6	5.1.1.6	Agency User Agreements	A NCJA (public) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions, **shall** be eligible for access to CJI.	1	Agency	Agency	Agency
108			"	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
109	5.1.1.6	5.1.1.6	"	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
110			"	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
111	5.1.1.6	5.1.1.6	"	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
112			"	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
113			"	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 5.5 Location and New Requirement	Ver 5.6 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
114	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
115	5.1.1.7	5.1.1.7	Outsourcing Standards for Channelers	Channelers designated to request civil fingerprint-based background checks or noncriminal justice ancillary functions on behalf of a NCJA (public) or NCJA (private) for noncriminal justice functions **shall** be eligible for access to CJI.	1	Agency	Agency	Agency
116			"	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
117			"	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
118			"	Each Channeler that directly accesses CJI **shall** also allow the FBI to conduct periodic penetration testing.	1	Agency	Agency	Agency
119			"	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
120			"	...and **shall** be subject to the same extent of audit review as are local user agencies.	1	Agency	Agency	Agency
121	5.1.1.8	5.1.1.8	Outsourcing Standards for Non-Channelers	Contractors designated to perform noncriminal justice ancillary functions on behalf of a NCJA (public) or NCJA (private) for noncriminal justice functions **shall** be eligible for access to CJI.	1	Agency	Agency	Agency
122			"	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
123			"	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
124			"	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
125	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
126	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
127	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
128			"	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
129	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
130			"	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
131	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
132	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 5.5 Location and New Requirement	Ver 5.6 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				
133	5.2	5.2	Policy Area 2: Security Awareness Training	Basic security awareness training **shall** be required within six months of initial assignment and biennially thereafter, for all personnel who have access to CJI to include all personnel who have unescorted access to a physically secure location.	1	Both	Both	Both
	5.2.1.1	5.2.1.1	Level One Security Awareness Training	At a minimum, the following topics **shall** be addressed as baseline security awareness training for all personnel who have access to a physically secure location:				
134			"	1. Individual responsibilities and expected behavior with regard to being in the vacinity of CJI usage and/or terminals.	1	Both	Both	Both
135			"	2. Implications of noncompliance.	1	Both	Both	Both
136			"	3. Incident response (Identify points of contact and individual actions).	1	Both	Both	Both
137			"	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
	5.2.1.2	5.2.1.2	Level Two Security Awareness Training	In addition to 5.2.1.1 above, the following topics, at a minimum, shall be addressed as baseline security awareness training for all authorized personnel with access to CJI:				
138			"	1. Media Protection.	1	Both	Both	Both
139			"	2. Protect information subject to confidentiality concerns — hardcopy through destruction.	1	Both	Both	Both
140			"	3. Proper handling and marking of CJI.	1	Both	Both	Both
141			"	4. Threats, vulnerabilities, and risks associated with handling of CJI.	1	Both	Both	Both
142			"	5. Social engineering.	1	Both	Both	Both
143			"	6. Dissemination and destruction.	1	Both	Both	Both
	~~5.2.1.2~~ ***5.2.1.3***	5.2.1.3	Level Three Security Awareness Training	In addition to 5.2.1.1 and 5.2.1.2 above, the following topics, at a minimum, **shall** be addressed as baseline security awareness training for all authorized personnel with both physical and logical access to CJI:				
144			"	1. Rules that describe responsibilities and expected behavior with regard to information system usage.	1	Both	Both	Both
145			"	2. Password usage and management—including creation, frequency of changes, and protection.	1	Both	Both	Both
146			"	3. Protection from viruses, worms, Trojan horses, and other malicious code.	1	Both	Both	Both
147			"	4. Unknown e-mail/attachments.	1	Both	Both	Both
148			"	5. Web usage—allowed versus prohibited; monitoring of user activity.	1	Both	Both	Both
149			"	6. Spam.	1	Both	Both	Both
150			"	7. Physical Security—increases in risks to systems and data.	1	Both	Both	Both
151			"	8. Handheld device security issues—address both physical and wireless security issues.	1	Both	Both	Both
152			"	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
153			"	10. Laptop security—address both physical and information security issues.	1	Both	Both	Both
154			"	11. Personally owned equipment and software—state whether allowed or not (e.g., copyrights).	1	Both	Both	Both
155			"	12. Access control issues—address least privilege and separation of duties.	1	Both	Both	Both
156			"	13. Individual accountability—explain what this means in the agency.	1	Both	Both	Both
157			"	14. Use of acknowledgement statements—passwords, access to systems and data, personal use and gain.	1	Both	Both	Both

	Ver 5.5 Location and New Requirement	Ver 5.6 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
158	~~5.2.1.2~~ ***5.2.1.3***	5.2.1.3	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
159			"	16. Protect information subject to confidentiality concerns—in systems, archived, on backup media, and until destroyed.	1	Both	Both	Both
160			"	17. Threats, vulnerabilities, and risks associated with accessing CJIS Service systems and services.	1	Both	Both	Both
	~~5.2.1.3~~ ***5.2.1.4***	5.2.1.4	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.):				
161			"	1. Protection from viruses, worms, Trojan horses, and other malicious code—scanning, updating definitions.	1	Both	Both	Both
162			"	2. Data backup and storage—centralized or decentralized approach.	1	Both	Both	Both
163			"	3. Timely application of system patches—part of configuration management.	1	Both	Both	Both
164			"	4. Access control measures.	1	Both	Both	Both
165			"	5. Network infrastructure protection measures.	1	Both	Both	Both
	5.2.2	5.2.2	Security Training Records	Records of individual basic security awareness training and specific information system security training **shall** be:				
166				- documented	1	Both	Both	Both
167				- kept current	1	Both	Both	Both
168				- maintained by the CSO/SIB/Compact Officer	1	Both	Both	Both

	Ver 5.5 Location and New Requirement	Ver 5.6 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				
169	5.3	5.3	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
170			"	...(ii) track, document, and report incidents to appropriate agency officials and/or authorities.	1	Both	Both	Both
171			"	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
172	5.3.1	5.3.1	Reporting Security Events	The agency **shall** promptly report incident information to appropriate authorities.	1	Both	Both	Both
173			"	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
174			"	Formal event reporting and escalation procedures **shall** be in place.	1	Both	Both	Both
175			"	Wherever feasible, the agency **shall** employ automated mechanisms to assist in the reporting of security incidents.	2	Both	Both	Both
176			"	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
	5.3.1.1.1	5.3.1.1.1	FBI CJIS Division Responsibilities	The FBI CJIS Division **shall**:				
177			"	1. Manage and maintain the CJIS Division's Computer Security Incident Response Capability (CSIRC).	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
178			"	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
179			"	3. Ensure additional resources for all incidents affecting FBI CJIS Division controlled systems as needed.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
180			"	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
181			"	5. Track all reported incidents and/or trends.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
182			"	6. Monitor the resolution of all incidents.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
	5.3.1.1.2	5.3.1.1.2	CSA ISO Responsibilities	The CSA ISO **shall**:				
183			"	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
184			"	2. Identify individuals who are responsible for reporting incidents within their area of responsibility.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
185	5.3.1.1.2	5.3.1.1.2	"	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
186			"	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
187			"	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
188			"	6. Act as a single POC for their jurisdictional area for requesting incident response assistance.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO

	Ver 5.5 Location and New Requirement	Ver 5.6 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
189	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
190			"	Responsibilities and procedures **shall** be in place to handle security events and weaknesses effectively once they have been reported.	1	Both	Both	Both
191	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
192			"	Wherever feasible, the agency **shall** employ automated mechanisms to support the incident handling process.	2	Both	Both	Both
193	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 i	1	Both	Both	Both
194	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
195	5.3.4	5.3.4	Incident Monitoring	The agency **shall** track and document security incidents on an ongoing basis.	1	Both	Both	Both
196			"	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 5.5 Location and New Requirement	Ver 5.6 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								
197	5.4	5.4	Policy Area 4:Auditing and Accountability	Agencies **shall** implement audit and accountability controls to increase the probability of authorized users conforming to a prescribed pattern of behavior.	1	Both	Both	Service Provider
198			"	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	Service Provider	Service Provider
199	5.4.1	5.4.1	Auditable Events and Content (Information Systems)	The agency's information system **shall** generate audit records for defined events.	1	Both	Both	Service Provider
200			"	The agency **shall** specify which information system components carry out auditing activities.	1	Both	Both	Service Provider
201			"	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
202			"	The agency **shall** periodically review and update the list of agency-defined auditable events.	2	Both	Both	Service Provider
203			"	In the event an agency does not use an automated system, manual recording of activities **shall** still take place.	1	Both	Both	Service Provider
	5.4.1.1	5.4.1.1	Events	The following events **shall** be logged:				
204			"	1. Successful and unsuccessful system log-on attempts.	1	Both	Both	Service Provider
205			"	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
206			"	3. Successful and unsuccessful attempts to change account passwords.	1	Both	Both	Service Provider
207			"	4. Successful and unsuccessful actions by privileged accounts.	1	Both	Both	Service Provider
208			"	5. Successful and unsuccessful attempts for users to access, modify, or destroy the audit log file.	1	Both	Both	Service Provider
	5.4.1.1.1	5.4.1.1.1	Content	The following content **shall** be included with every audited event:				
209			"	1. Date and time of the event.	1	Both	Both	Service Provider
210			"	2.The component of the information system (e.g., software component, hardware component) where the event occurred.	1	Both	Both	Service Provider
211			"	3. Type of event.	1	Both	Both	Service Provider
212			"	4. User/subject identity.	1	Both	Both	Service Provider
213			"	5. Outcome (success or failure) of the event.	1	Both	Both	Service Provider
214	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
215	5.4.3	5.4.3	Audit Monitoring, Analysis, and Reporting	The responsible management official **shall** designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions.	2	Both	Both	Both
216			"	Audit review/analysis **shall** be conducted at a minimum once a week.	2	Both	Both	Both

	Ver 5.5 Location and New Requirement	Ver 5.6 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
217	5.4.3	5.4.3	Audit Monitoring, Analysis, and Reporting (continued)	The agency **shall** increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to agency operations, agency assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.	2	Both	Both	Both
218	5.4.4	5.4.4	Time Stamps	The agency's information system **shall** provide time stamps for use in audit record generation.	2	Both	Both	Service Provider
219			"	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
220			"	The agency **shall** synchronize internal information system clocks on an annual basis.	2	Both	Both	Service Provider
221	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
222	5.4.6	5.4.6	Audit Record Retention	The agency **shall** retain audit records for at least one (1) year.	1	Both	Both	Service Provider
223			"	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
224	5.4.7	5.4.7	Logging NCIC and III Transactions	A log **shall** be maintained for a minimum of one (1) year on all NCIC and III transactions.	1	Both	Both	Service Provider
225			"	The III portion of the log **shall** clearly identify both the operator and the authorized receiving agency.	1	Agency	Agency	Agency
226			"	III logs **shall** also clearly identify the requester and the secondary recipient.	1	Agency	Agency	Agency
227			"	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 5.5 Location and New Requirement	Ver 5.6 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								
228	5.5.1	5.5.1	Account Management	The agency **shall** manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts.	1	Agency	Both	Both
229			"	The agency **shall** validate information system accounts at least annually and…	1	Agency	Both	Both
230			"	...and **shall** document the validation process.	2	Agency	Both	Both
231			"	The agency **shall** identify authorized users of the information system and specify access rights/privileges.	1	Agency	Both	Both
			"	The agency **shall** grant access to the information system based on:				
232			"	1. Valid need-to-know/need-to-share that is determined by assigned official duties.	1	Agency	Both	Both
233			"	2. Satisfaction of all personnel security criteria.	1	Agency	Both	Both
			"	The agency responsible for account creation **shall** be notified when:				
234			"	1. A user's information system usage or need-to-know or need-to-share changes.	1	Agency	Both	Both
235			"	2. A user is terminated or transferred or associated accounts are removed, disabled, or otherwise secured.	1	Agency	Both	Both
236	5.5.2	5.5.2	Access Enforcement	The information system **shall** enforce assigned authorizations for controlling access to the system and contained information.	1	Agency	Both	Both
237			"	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
238			"	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
239	5.5.2.1	5.5.2.1	Least Privilege	The agency **shall** approve individual access privileges and…	1	Agency	Both	Both
240			"	…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
241			"	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
242			"	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
243			"	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
244	5.5.2.2	5.5.2.2	System Access Control	Access control mechanisms to enable access to CJI **shall** be restricted by object (e.g., data set, volumes, files, records) including the ability to read, write, or delete the objects.	2	Agency	Both	Both
			"	Access controls **shall** be in place and operational for all IT systems to:				
245			"	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
246			"	(1. continued) Agencies **shall** document the parameters of the operational business needs for multiple concurrent active sessions.	2	Agency	Both	Both
247			"	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 5.5 Location and New Requirement	Ver 5.6 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
	5.5.2.3	5.5.2.3	Access Control Criteria	Agencies **shall** control access to CJI based on one or more of the following:				
248			"	1. Job assignment or function (i.e., the role) of the user seeking access.	1	Agency	Both	Both
249			"	2. Physical location.	1	Agency	Both	Both
250			"	3. Logical location.	1	Agency	Both	Both
251			"	4. Network addresses (e.g., users from sites within a given agency may be permitted greater access than those from outside).	1	Agency	Both	Both
252			"	5. Time-of-day and day-of-week/month restrictions.	1	Agency	Both	Both
	5.5.2.4	5.5.2.4	Access Control Mechanisms	When setting up access controls, agencies **shall** use one or more of the following mechanisms:				
253			"	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.	1	Agency	Both	Both
254			"	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.	1	Agency	Both	Both
255			"	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).	1	Agency	Both	Both
256			"	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.	1	Agency	Both	Both
257	5.5.3	5.5.3	Unsuccessful Login Attempts	Where technically feasible, the system **shall** enforce a limit of no more than 5 consecutive invalid access attempts by a user (attempting to access CJI or systems with access to CJI).	2	Agency	Both	Both
258			"	The system **shall** automatically lock the account/node for a 10 minute time period unless released by an administrator.	2	Agency	Both	Both
259	5.5.4	5.5.4	System Use Notification	The information system **shall** display an approved system use notification message, before granting access, informing potential users of various usages and monitoring rules.	2	Agency	Both	Both
			"	The system use notification message **shall**, at a minimum, provide the following information:				
260			"	1. The user is accessing a restricted information system.	2	Agency	Both	Both
261			"	2. System usage may be monitored, recorded, and subject to audit.	2	Agency	Both	Both
262			"	3. Unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties.	2	Agency	Both	Both
263			"	4. Use of the system indicates consent to monitoring and recording.	2	Agency	Both	Both
264			"	The system use notification message **shall** provide appropriate privacy and security notices (based on associated privacy and security policies or summaries) and…	2	Agency	Both	Both
265			"	...and remain on the screen until the user acknowledges the notification and takes explicit actions to log on to the information system.	2	Agency	Both	Both
266			"	Privacy and security policies **shall** be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.	2	Agency	Both	Both

	Ver 5.5 Location and New Requirement	Ver 5.6 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
267	5.5.5	5.5.5	Session Lock	The information system **shall** prevent further access to the system by initiating a session lock after a maximum of 30 minutes of inactivity, and…	2	Agency	Both	Both
268			"	...and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures.	2	Agency	Both	Both
269			"	Users **shall** directly initiate session lock mechanisms to prevent inadvertent viewing when a device is unattended.	2	Agency	Both	Both
270	5.5.6	5.5.6	Remote Access	The agency **shall** authorize, monitor, and control all methods of remote access to the information system.	1	Agency	Both	Both
271			"	The agency **shall** employ automated mechanisms to facilitate the monitoring and control of remote access methods.	1	Agency	Both	Both
272			"	The agency **shall** control all remote accesses through managed access control points.	1	Agency	Both	Both
273			"	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
[redacted]			"	Virtual escorting of privileged functions is permitted only when all the following conditions are met:	[redacted]	[redacted]	[redacted]	[redacted]
274			"	1. The session **shall** be monitored at all times by an authorized escort.	1	Agency	Both	Both
275			"	2. The escort **shall** be familiar with the system/area in which the work is being performed.	1	Agency	Both	Both
276			"	3. The escort **shall** have the ability to end the session at any time.	1	Agency	Both	Both
277			"	4. The remote administrative personnel connection **shall** be via an encrypted (FIPS 140-2 certified) path.	1	Agency	Both	Both
278			"	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	1	Agency	Both	Both
279	5.5.6.1	5.5.6.1	Personally Owned Information Systems	A personally owned information system **shall not** be authorized to access, process, store or transmit CJI unless the agency has established and documented the specific terms and conditions for personally owned information system usage.	1	Agency	Both	Both
280			"	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
281	5.5.6.2	5.5.6.2	Publicly Accessible Computers	Publicly accessible computers **shall not** be used to access, process, store or transmit CJI. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.	1	Agency	Both	Both

	Ver 5.5 Location and New Requirement	Ver 5.6 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								
282	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
283	5.6.1	5.6.1	Identification Policy and Procedures	Each person who is authorized to store, process, and/or transmit CJI **shall** be uniquely identified.	1	Agency	Both	Both
284			"	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
285			"	Agencies **shall** require users to identify themselves uniquely before the user is allowed to perform any actions on the system.	1	Agency	Both	Both
286			"	Agencies **shall** ensure that all user IDs belong to currently authorized users.	1	Agency	Both	Both
287			"	Identification data **shall** be kept current by adding new users and disabling and/or deleting former users.	1	Agency	Both	Both
288	5.6.1.1	5.6.1.1	Use of Originating Agency Identifiers in Transactions and Information Exchanges	An FBI authorized originating agency identifier (ORI) **shall** be used in each transaction on CJIS systems in order to identify the sending agency and to ensure the proper level of access for each transaction.	1	Agency	Agency	Agency
289			"	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
290			"	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
291			"	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
292	5.6.2	5.6.2	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
293			"	The authentication strategy **shall** be part of the agency's audit for policy compliance.	2	Agency	Agency	Agency
294			"	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
295			"	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
296	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
297	5.6.2.1.1	5.6.2.1.1	Password	Agencies **shall** follow the secure password attributes, below, to authenticate an individual's unique ID.	1	Agency	Both	Both
			"	Passwords **shall**:				
298			"	1. Be a minimum length of eight (8) characters on all systems.	1	Agency	Both	Both
299			"	2. Not be a dictionary word or proper name.	1	Agency	Both	Both
300			"	3. Not be the same as the Userid.	1	Agency	Both	Both
301			"	4. Expire within a maximum of 90 calendar days.	1	Agency	Both	Both
302			"	5. Not be identical to the previous ten (10) passwords.	2	Agency	Both	Both
303			"	6. Not be transmitted in the clear outside the secure location.	1	Agency	Both	Both
304			"	7. Not be displayed when entered.	1	Agency	Both	Both

	Ver 5.5 Location and New Requirement	Ver 5.6 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
305	5.6.2.1.2	5.6.2.1.2	Personal Identification Number (PIN)	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).	1	Agency	Both	Both
				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.				
306				1. Be a minimum length of six (6) digits.	1	Agency	Both	Both
307				2. Have no repeating digits (i.e., 112233).	1	Agency	Both	Both
308				3. Have no sequential patterns (i.e., 123456).	1	Agency	Both	Both
309				4. Not be the same as the Userid.	1	Agency	Both	Both
310				5. Expire within a maximum of 365 days.	1	Agency	Both	Both
311				6. Not be identical to the previous three (3) PINs.	1	Agency	Both	Both
312				7. Not be transmitted in the clear outside the secure location.	1	Agency	Both	Both
313				8. Not be displayed when entered.	1	Agency	Both	Both
		5.6.2.1.3	***One-time Passwords (OTP)***	***When agencies implement the use of an OTP as authenticator, the OTP shall meet the requirements described below.***				
314			***"***	***a. Be a minimum of six (6) randomly generated characters.***	1	Agency	Both	Both
315			***"***	***b. Be valid for a single session.***	1	Agency	Both	Both
316			***"***	***c. If not used, expire within a maximum of five (5) minutes after issuance.***	1	Agency	Both	Both
	5.6.2.2	5.6.2.2	Advanced Authentication	When user-based certificates are used for authentication purposes, they **shall**:				
317			"	1. Be specific to an individual user and not to a particular device.	1	Agency	Both	Both
318			"	2. Prohibit multiple users from utilizing the same certificate.	1	Agency	Both	Both
319			"	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
320	5.6.2.2.1	5.6.2.2.1	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...	1	Agency	Both	Both
321			"	... or when the user has no ability to conduct transactional activities on state and national repositories, applications, or services (i.e. indirect access).	1	Agency	Both	Both
322			"	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
323			"	The two authentication factors **shall** be unique (i.e. password/token or biometric/password but not password/password or token/token).	1	Agency	Both	Both
324			"	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.	1	Agency	Both	Both
325	5.6.3	5.6.3	Identifier and Authenticator Management	The agency **shall** establish identifier and authenticator management processes.	1	Agency	Both	Both
	5.6.3.1	5.6.3.1	Identifier Management	In order to manage user identifiers, agencies **shall**:				
326			"	1. Uniquely identify each user.	1	Agency	Both	Both
327			"	2. Verify the identity of each user.	1	Agency	Both	Both
328			"	3. Receive authorization to issue a user identifier from an appropriate agency official.	1	Agency	Both	Both
329			"	4. Issue the user identifier to the intended party.	1	Agency	Both	Both
330			"	5. Disable the user identifier after a specified period of inactivity.	1	Agency	Both	Both
331			"	6. Archive user identifiers.	1	Agency	Both	Both
	5.6.3.2	5.6.3.2	Authenticator Management	In order to manage information system authenticators, agencies **shall**:				
332			"	1. Define initial authenticator content.	1	Agency	Both	Both
333			"	2. Establish administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators.	1	Agency	Both	Both
334			"	3. Change default authenticators upon information system installation.	1	Agency	Both	Both
335			"	4. Change/refresh authenticators periodically.	1	Agency	Both	Both

	Ver 5.5 Location and New Requirement	Ver 5.6 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
336	5.6.3.2	5.6.3.2	Authenticator Management (continued)	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.	1	Agency	Both	Both
	5.6.4	5.6.4	Assertions	Assertion mechanisms used to communicate the results of a remote authentication to other parties **shall** be:				
337			"	1. Digitally signed by a trusted entity (e.g., the identity provider).	1	Agency	Both	Both
338			"	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
339			"	Assertions generated by a verifier **shall** expire after 12 hours and…	1	Agency	Both	Both
340			"	...and **shall not** be accepted thereafter by the relying party.	1	Agency	Both	Both

	Ver 5.5 Location and New Requirement	Ver 5.6 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy Area 7 - Configuration Management								
341	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
342			"	...and **shall** specifically prohibit and/or restrict the use of specified functions, ports, protocols, and/or services.	1	Agency	Both	Both
343	5.7.1.2	5.7.1.2	Network Diagram	The agency **shall** ensure that a complete topological drawing depicting the interconnectivity of the agency network, to criminal justice information, systems and services is maintained in a current status.	1	Agency	Both	Both
			"	The network topological drawing **shall** include the following:				
344			"	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
345			"	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
346			"	3. “For Official Use Only” (FOUO) markings.	1	Agency	Both	Both
347			"	4. The agency name and date (day, month, and year) drawing was created or updated.	1	Agency	Both	Both
348	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 5.5 Location and New Requirement	Ver 5.6 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								
349	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
350			"	Procedures **shall** be defined for securely handling, transporting and storing media.	2	Agency	Agency	Agency
351	5.8.1	5.8.1	Media Storage and Access	The agency **shall** securely store electronic and physical media within physically secure locations or controlled areas.	1	Both	Both	Both
352			"	The agency **shall** restrict access to electronic and physical media to authorized individuals.	1	Both	Both	Both
353			"	If physical and personnel restrictions are not feasible then the data **shall** be encrypted per section 5.10.1.2.	1	Both	Both	Both
354	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
355	5.8.2.1	5.8.2.1	Electronic Media in Transit	Controls **shall** be in place to protect digital media containing CJI while in transport (physically moved from one location to another) to help prevent compromise of the data.	1	Agency	Agency	Agency
356			"	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
357	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
358	5.8.3	5.8.3	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
359			"	Inoperable electronic media **shall** be destroyed (cut up, shredded, etc.).	1	Agency	Agency	Agency
360			"	The agency **shall** maintain written documentation of the steps taken to sanitize or destroy electronic media.	2	Agency	Agency	Agency
361			"	Agencies **shall** ensure the sanitization or destruction is witnessed or carried out by authorized personnel.	1	Agency	Agency	Agency
362	5.8.4	5.8.4	Disposal of Physical Media	Physical media **shall** be securely disposed of when no longer required, using formal procedures.	1	Agency	Agency	Agency
363			"	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
364			"	Physical media **shall** be destroyed by shredding or incineration.	1	Agency	Agency	Agency
365			"	Agencies **shall** ensure the disposal or destruction is witnessed or carried out by authorized personnel.	1	Agency	Agency	Agency

	Ver 5.5 Location and New Requirement	Ver 5.6 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								
366	5.9	5.9	Policy Area 9: Physical Protection	Physical protection policy and procedures **shall** be documented and implemented to ensure CJI and information system hardware, software, and media are physically protected through access control measures.	2	Both	Both	Both
367	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
368			"	Security perimeters **shall** be defined, controlled and secured in a manner acceptable to the CSA or SIB.	1	Both	Both	Both
369	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
370			"	...or **shall** issue credentials to authorized personnel.	1	Both	Both	Both
371	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
372			"	...and **shall** verify individual access authorizations before granting access.	1	Both	Both	Both
373	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
374	5.9.1.5	5.9.1.5	Access Control for Display Medium	The agency **shall** control physical access to information system devices that display CJI and…	1	Both	Both	Both
375			"	...and **shall** position information system devices in such a way as to prevent unauthorized individuals from accessing and viewing CJI.	1	Both	Both	Both
376	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
377	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
378			"	The agency **shall** escort visitors at all times and monitor visitor activity.	1	Both	Both	Both
379	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
380	5.9.2	5.9.2	Controlled Area	If an agency cannot meet all of the controls required for establishing a physically secure location, but has an operational need to access or store CJI, the agency **shall** designate an area, a room, or a storage container, as a "controlled area" for the purpose of day-to-day CJI access or storage.	1	Both	Both	Both
			"	The agency **shall**, at a minimum:				
381			"	1. Limit access to the controlled area during CJI processing times to only those personnel authorized by the agency to access or view CJI.	1	Both	Both	Both
382			"	2. Lock the area, room, or storage container when unattended.	1	Both	Both	Both
383			"	3. Position information system devices and documents containing CJI in such a way as to prevent unauthorized individuals from access and view.	1	Both	Both	Both
384			"	4. Follow the encryption requirements found in section 5.10.1.1.2 for electronic storage (i.e. data "at rest") of CJI.	1	Both	Both	Both

	Ver 5.5 Location and New Requirement	Ver 5.6 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy Area 10 - Systems and Communications Protection and Information Integrity								
385	5.10.1	5.10.1	Information Flow Enforcement	The network infrastructure **shall** control the flow of information between interconnected systems.	1	Both	Service Provider	Service Provider
	5.10.1.1	5.10.1.1	Boundary Protection	The agency **shall**:				
386			"	1. Control access to networks processing CJI.	1	Both	Service Provider	Service Provider
387			"	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
388			"	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
389			"	4. Employ tools and techniques to monitor network events, detect attacks, and provide identification of unauthorized use.	1	Both	Service Provider	Service Provider
390			"	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 **shall** "fail closed" vs. "fail open").	1	Both	Service Provider	Service Provider
391			"	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
	5.10.1.2		~~Encryption~~	~~1. Encryption **shall** be a minimum of 128 bit.~~				
392		5.10.1.2.1	***Encryption for CJI in Transit***	~~2.~~ When CJI is transmitted outside the boundary of the physically secure location, the data **shall** be immediately protected via ~~cryptographic mechanisms (~~encryption~~)~~.	1	Both	Service Provider	Service Provider
393			"	***When encryption is employed, the cryptographic module used shall be FIPS 140-2 certified and …***	1	Both	Service Provider	Service Provider
394			"	***… and use a symmetric cipher key strength of at least 128 bit strength to protect CJI.***	1	Both	Service Provider	Service Provider
			"	b) Encryption **shall not** be required if the transmission medium meets all of the following requirements:				
395			"	i. The agency owns, operates, manages, or protects the medium.	1	Agency	Agency	Agency
396			"	ii. Medium terminates within physically secure locations at both ends with no interconnections between.	1	Agency	Agency	Agency
397			"	iii. Physical access to the medium is controlled by the agency using the requirements in Section 5.9.1 and 5.12.	1	Agency	Agency	Agency
398			"	iv. Protection includes safeguards (e.g. acoustic, electric, electromagnetic, and physical) and if feasible countermeasures (e.g. alarms, notifications) to permit its use for the tranmission of unencrypted information through an area of lesser classification or control.	1	Agency	Agency	Agency
399			"	v. With approval of the CSO.	1	Agency	Agency	Agency
400		5.10.1.2.2	***Encryption for CJI at Rest***	~~3.~~ When CJI is at rest (i.e. stored electronically) outside the boundary of the physically secure location, the data **shall** be protected via ~~cryptographic mechanisms (~~encryption~~)~~.	1	Both	Service Provider	Service Provider
401			"	***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
402			"	***… or use a symmetric cipher that is FIPS 197 certified (AES) and at least 256 bit strength.***	1	Both	Service Provider	Service Provider
			"	a) When agencies implement encryption on CJI at rest, the passphrase to unlock the cipher **shall** meet the following requirements:				

	Ver 5.5 Location and New Requirement	Ver 5.6 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
403	5.10.1.2	***5.10.1.2.2***	***Encryption for CJI at Rest (continued)***	i. Be at least 10 characters	1	Both	Service Provider	Service Provider
404			"	ii. Not be a dictionary word	1	Both	Service Provider	Service Provider
405			"	iii. Include at least one (1) upper case letter, one (1) lower case letter, one (1) number, and one (1) special character	1	Both	Service Provider	Service Provider
406			"	iv. Be changed when previously authorized personnel no longer require access	1	Both	Service	Service
407			"	b) Multiple files maintained in the same unencrypted folder **shall** have separate and distinct passphrases.	1	Both	Service Provider	Service Provider
408			"	b) All audit requirements found in Section 5.4.1 Auditable Events and Content (Information Systems) **shall** be applied.	1	Both	Service Provider	Service Provider
				~~4. When encryption is employed, the cryptographic module used **shall** be certified to meet FIPS 140-2 standards.~~				
409		***5.10.1.2.3***	***Public Key Infrastructure (PKI) Technology***	~~5.~~ 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	1	Both	Service Provider	Service Provider
			"	Registration to receive a public key certificate **shall**:				
410			"	a) Include authorization by a supervisor or a responsible official.	1	Both	Service Provider	Service Provider
411			"	b) Be accomplished by a secure process that verifies the identity of the certificate holder.	1	Both	Service Provider	Service Provider
412			"	c) Ensure the certificate is issued to the intended party.	1	Both	Service Provider	Service Provider
413	5.10.1.3	5.10.1.3	Intrustion Detection Tools and Techniques	The agency **shall** implement network-based and/or host-based intrusion detection tools.	1	Both	Service Provider	Service Provider
			"	The CSA/SIB **shall**, in addition:				
414			"	1. Monitor inbound and outbound communications for unusual or unauthorized activities.	1	Both	Service Provider	Service Provider
415			"	2. Send individual intrusion detection logs to a central logging facility where correlation and analysis will be accomplished as a system wide intrusion detection effort.	1	Both	Service Provider	Service Provider
416			"	3. Employ automated tools to support near-real-time analysis of events in support of detecting system-level attacks.	1	Both	Service Provider	Service Provider
	5.10.1.4	5.10.1.4	Voice over Internet Protocol	In addition to the security controls described in this document, the following additional controls **shall** be implemented when an agency deploys VoIP within a network that contains unencrypted CJI:				
417			"	1. Establish usage restrictions and implementation guidance for VoIP technologies.	1	Both	Service Provider	Service Provider
418			"	2. Document, monitor and control the use of VoIP within the agency.	1	Both	Service Provider	Service Provider
419			"	3. Utilize Virtual Local Area Network (VLAN) technology to segment VoIP traffic from data traffic.	1	Both	Service Provider	Service Provider
420	5.10.1.5	5.10.1.5	Cloud Computing	The metadata derived from Criminal Justice Information **shall not** be used by and Cloud Provider for any purposes.	1	Service Provider	Service Provider	Service Provider
421			"	The Cloud Provider **shall be prohibited from** scanning any email or data files for the purpose of building analytics, data mining, advertising, or improving the services provided.	1	Service Provider	Service Provider	Service Provider
422	***New 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

	Ver 5.5 Location and New Requirement	Ver 5.6 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
423	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
424			"	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
	5.10.3.2	5.10.3.2	Virtualization	In addition to the security controls described in this policy, the following additional controls **shall** be implemented in a virtual environment:				
425			"	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
426			"	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
427			"	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
428			"	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
	New 5.10.3.2		"	The following additional technical security controls **shall** be applied in virtual environments where CJI is comingled with non-CJI:				
429			"	1. Encrypt CJI when stored in a virtualized environment where CJI is comingled with non-CJI or segregate and store unencrypted CJI within its own secure VM.	1	Both	Service Provider	Service Provider
430			"	2. Encrypt network traffic within the virtual environment.	1	Both	Service Provider	Service Provider
431	5.10.4.1	5.10.4.1	Patch Management	The agency **shall** identify applications, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws.	1	Both	Service Provider	Service Provider
432			"	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
433			"	Patch requirements discovered during security assessments, continuous monitoring or incident response activities **shall** also be addressed expeditiously.	1	Both	Service Provider	Service Provider
434	5.10.4.2	5.10.4.2	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
435			"	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
436	5.10.4.2	5.10.4.2	Malicious Code Protection (continued)	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
437			"	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
438	5.10.4.3	5.10.4.3	Spam and Spyware Protection	The agency **shall** implement spam and spyware protection.	2	Both	Service Provider	Service Provider
			"	The agency **shall**:				
439			"	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

	Ver 5.5 Location and New Requirement	Ver 5.6 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
440	5.10.4.3	5.10.4.3	Spam and Spyware Protection (continued)	2. Employ spyware protection at workstations, servers and mobile computing devices on the network.	2	Both	Service Provider	Service Provider
441			"	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
	5.10.4.4	5.10.4.4	Security Alerts and Advisories	The agency **shall**:				
442			"	1. Receive information system security alerts/advisories on a regular basis.	2	Both	Service Provider	Service Provider
443			"	2. Issue alerts/advisories to appropriate personnel.	2	Both	Service Provider	Service Provider
444			"	3. Document the types of actions to be taken in response to security alerts/advisories.	2	Both	Service Provider	Service Provider
445			"	4. Take appropriate actions in response.	2	Both	Service Provider	Service Provider
446			"	5. Employ automated mechanisms to make security alert and advisory information available throughout the agency as appropriate.	2	Both	Service Provider	Service Provider
447	5.10.4.5	5.10.4.5	Information Input Restrictions	The agency **shall** restrict the information input to any connection to FBI CJIS services to authorized personnel only.	1	Agency	Agency	Agency

	Ver 5.5 Location and New Requirement	Ver 5.6 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								
448	5.11.1.1	5.11.1.1	Triennial Compliance Audits by the FBI CJIS Division	The CJIS Audit Unit (CAU) **shall** conduct a triennial audit of each CSA in order to verify compliance with applicable statutes, regulations and policies.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
449			"	This audit **shall** include a sample of CJAs and, in coordination with the SIB, the NCJAs.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
450			"	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
451	5.11.1.2	5.11.1.2	Triennial Security Audits by the FBI CJIS Division	This audit **shall** include a sample of CJAs and NCJAs.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
	5.11.2	5.11.2	Audits by the CSA	Each CSA **shall**:				
452			"	1. At a minimum, triennially audit all CJAs and NCJAs which have direct access to the state system in order to ensure compliance with applicable statutes, regulations and policies.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
453			"	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
454			"	3. Have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
455	***New*** ***5.11.2***		"	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
456	5.11.3	5.11.3	Special Security Inquiries and Audits	All agencies having access to CJI **shall** permit an inspection team to conduct an appropriate inquiry and audit of any alleged security violations.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
457			"	The inspection team **shall** be appointed by the APB and **shall** include at least one representative of the CJIS Division.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
458			"	All results of the inquiry and audit **shall** be reported to the APB with appropriate recommendations.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO

	Ver 5.5 Location and New Requirement	Ver 5.6 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy Area 12 - Personnel Security								
459	5.12.1.1	5.12.1.1	Minimum Screening Requirements for Individuals Requiring Access to CJI	1. To verify identification, a state of residency and national fingerprint-based record checks **shall** be conducted within 30 days of assignment for all personnel who have direct access to CJI and those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI.	1	Agency	Agency	Agency
460			"	However, if the person resides in a different state than that of the assigned agency, the agency **shall** conduct state (of the agency) and national fingerprint-based record checks and execute a NLETS CHRI IQ/FQ/AQ query using purpose code C, E, or J depending on the circumstances.	1	Agency	Agency	Agency
461			"	When appropriate, the screening **shall** be consistent with (i) 5 CFR 731.106; and/or (ii) Office of Personnel Management policy, regulations, and guidance; and/or (iii) agency policy, regulations, and guidance.	1	Agency	Agency	Agency
462			"	2. All requests for access **shall** be made as specified by the CSO.	1	Agency	Agency	Agency
463			"	All CSO designees **shall** be from an authorized criminal justice agency.	1	Agency	Agency	Agency
464			"	3. If a felony conviction of any kind exists, the hiring authority in the Interface Agency **shall** deny access to CJI.	1	Agency	Agency	Agency
465			"	4. If a record of any other kind exists, access to CJI **shall not** be granted until the CSO or his/her designee reviews the matter to determine if access is appropriate.	1	Agency	Agency	Agency
466			"	5. If the person appears to be a fugitive or has an arrest history without conviction, the CSO or his/her designee **shall** review the matter to determine if access to CJI is appropriate.	1	Agency	Agency	Agency
467			"	6. If the person is employed by a noncriminal justice agency, the CSO or his/her designee, and, if applicable, the appropriate board maintaining management control, **shall** review the matter to determine if CJI access is appropriate.	1	Agency	Agency	Agency
468			"	7. If the person already has access to CJI and is subsequently arrested and or convicted, continued access to CJI **shall** be determined by the CSO.	1	Agency	Agency	Agency
469			"	8. If the CSO or his/her designee determines that access to CJI by the person would not be in the public interest, access **shall** be denied and the person's appointing authority shall be notified in writing of the access denial.	1	Agency	Agency	Agency
470			"	8. If the CSO or his/her designee determines that access to CJI by the person would not be in the public interest, access shall be denied and the person's appointing authority **shall** be notified in writing of the access denial.	1	Agency	Agency	Agency
471			"	9. Support personnel, contractors, and custodial workers with access to physically secure locations or controlled areas (during CJI processing) **shall** be subject to a state and national fingerprint-based record check unless these individuals are escorted by authorized personnel at all times.	1	Agency	Agency	Agency
472	5.12.1.2	5.12.1.2	Personnel Screening for Contractors and Vendors	In addition to meeting the requirements in paragraph 5.12.1.1, contractors and vendors **shall** meet the following requirements:	1	Agency	Agency	Agency
473			"	1. Prior to granting access to CJI, the CGA on whose behalf the Contractor is retained **shall** verify identification via a state of residency and national fingerprint-based record checks.	1	Agency	Agency	Agency
474			"	However, if the person resides in a different state than that of the assigned agency, the agency **shall** conduct state (of the agency) and national fingerprint-based record checks and execute a NLETS CHRI IQ/FQ/AQ query using purpose code C, E, or J depending on the circumstances.	1	Agency	Agency	Agency
475			"	2. If a record of any kind is found, the CGA **shall** be formally notified, and…	1	Agency	Agency	Agency
476			"	...and system access **shall** be delayed pending review of the criminal history record information.	1	Agency	Agency	Agency

	Ver 5.5 Location and New Requirement	Ver 5.6 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
477	5.12.1.2	5.12.1.2	Personnel Screening for Contractors and Vendors (continued)	The CGA **shall** in turn notify the Contractor-appointed Security Officer.	1	Agency	Agency	Agency
478			"	3. When identification of the applicant with a criminal history has been established by fingerprint comparison, the CGA or the CJA (if the CGA does not have the authority to view CHRI) **shall** review the matter.	1	Agency	Agency	Agency
479			"	4. A Contractor employee found to have a criminal record consisting of felony conv	1	Agency	Agency	Agency
480			"	5. Applicants **shall** also be disqualified on the basis of confirmations that arrest warrants are outstanding for such applicants.	1	Agency	Agency	Agency
481			"	6. The CGA **shall** maintain a list of personnel who have been authorized access to CJI and…	1	Agency	Agency	Agency
482			"	6. ...and **shall**, upon request, provide a current copy of the access list to the CSO.	1	Agency	Agency	Agency
483	5.12.2	5.12.2	Personnel Termination	The agency, upon termination of individual employment, **shall** immediately terminate access to CJI.	1	Both	Both	Both
484	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
485	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 5.5 Location and New Requirement	Ver 5.6 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								
	5.13	5.13	Mobile Devices	The agency **shall**:				
486			"	(i) establish usage restrictions and implementation guidance for mobile devices;	1	Agency	Agency	Agency
487			"	(ii) authorize, monitor, control wireless access to the information system.	1	Agency	Agency	Agency
488	5.13.1.1	5.13.1.1	802.11 Wireless Protocols	Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) cryptographic algorithms, used by all pre-80.11i protocols, do not meet the requirements for FIPS 140-2 and **shall not** be used.	1	Agency	Agency	Agency
489			"	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:				
490			"	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
491			"	2. Maintain a complete inventory of all Access Points (APs) and 802.11 wireless devices.	1	Agency	Agency	Agency
492			"	3. Place APs in secured areas to prevent unauthorized physical access and user manipulation.	1	Agency	Agency	Agency
493			"	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
494			"	5. Enable user authentication and encryption mechanisms for the management interface of the AP.	1	Agency	Agency	Agency
495			"	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
496			"	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
497			"	8. Change the default service set identifier (SSID) in the APs.	1	Agency	Agency	Agency
498			"	Disable the broadcast SSID feature so that the client SSID must match that of the AP.	1	Agency	Agency	Agency
499			"	Validate that the SSID character string does not contain any agency identifiable information (division, department, street, etc.) or services.	1	Agency	Agency	Agency
500			"	9. Enable all security features of the wireless product, including the cryptographic authentication, firewall, and other privacy features.	1	Agency	Agency	Agency
501			"	10. Ensure that encryption key sizes are at least 128-bits and…	1	Agency	Agency	Agency
502			"	...and the default shared keys are replaced by unique keys.	1	Agency	Agency	Agency
503			"	11. Ensure that the ad hoc mode has been disabled.	1	Agency	Agency	Agency
504			"	12. Disable all nonessential management protocols on the APs. Disable non-FIPS compliant secure access to the managment interface.	1	Agency	Agency	Agency
505			"	13. Ensure all management access and authentication occurs via FIPS compliant secure protocols (e.g. SFTP, HTTPS, SNMP over TLS, etc.). Disable non-FIPS compliant secure access to the managment interface.	1	Agency	Agency	Agency
506			"	14. Enable logging (if supported) and…	1	Agency	Agency	Agency
507			"	...and review the logs on a recurring basis per local policy.	1	Agency	Agency	Agency
508			"	At a minimum logs **shall** be reviewed monthly.	1	Agency	Agency	Agency

	Ver 5.5 Location and New Requirement	Ver 5.6 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
509	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
510			"	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
511	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
512	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
	~~5.13.8~~ ***5.13.1.4***	5.13.1.4	Mobile Hotspots	When an agency allows mobile devices that are approved to access or store CJI to function as a Wi-Fi hotspot connecting to the Internet, they **shall** be configured:				
513			"	1. Enable encryption on the hotspot	1	Agency	Agency	Agency
514	***New*** ***5.13.1.4***		"	2. Change the hotspot's default SSID	1	Agency	Agency	Agency
515			"	a. Ensure the hotspot SSID does not identify the device make/model or agency ownership	1	Agency	Agency	Agency
516			"	3. Create a wireless network password (Pre-shared key)	1	Agency	Agency	Agency
517			"	4. Enable the hotspot's port filtering/blocking features if present	1	Agency	Agency	Agency
518	~~5.13.8~~ ***5.13.1.4***		"	5. Only allow connections from agency controlled devices	1	Agency	Agency	Agency
519	***New*** ***5.13.1.4***		"	OR 1. Have a MDM solution to provide the same security as identified in 1 - 5 above.	1	Agency	Agency	Agency
520	5.13.2	5.13.2	Mobile Device Management (MDM)	Devices that have had any unauthorized changes made to them (including but not limited to being rooted or jailbroken) **shall not** be used to process, store, or transmit CJI at any time.	1	Agency	Agency	Agency
			"	Agencies **shall** implement the following controls when allowing CJI access from devices running limited feature operating system:				
521			"	1. Ensure that CJI is only transferred between CJI authorized applications and storage areas of the device.	1	Agency	Agency	Agency
522			"	2. MDM with centralized administration configured and implemented to perform at least the:	1	Agency	Agency	Agency
523			"	i. Remote locking of the device	1	Agency	Agency	Agency
524			"	ii. Remote wiping of the device	1	Agency	Agency	Agency
525			"	iii. Setting and locking device configuration	1	Agency	Agency	Agency
526			"	iv. Detection of "rooted" and "jailbroken" devices	1	Agency	Agency	Agency
527			"	v. Enforcement of folder or disk level encryption	1	Agency	Agency	Agency
528			"	vi. Application of mandatory policy settings on the device	1	Agency	Agency	Agency
529			"	vii. Detection of unauthorized configurations	1	Agency	Agency	Agency
530			"	viii. Detection of unauthorized software or applications	1	Agency	Agency	Agency
531			"	ix. Ability to determine location of agency controlled devices	1	Agency	Agency	Agency
532			"	x. Prevention of unpatched devices from accessing CJI or CJI systems	1	Agency	Agency	Agency
533			"	xi. Automatic device wiping after a specified number of failed access attempts	1	Agency	Agency	Agency
	5.13.3	5.13.3	Wireless Device Risk Mitigations	Organizations **shall**, as a minimum, ensure that wireless devices:				
534			"	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

	Ver 5.5 Location and New Requirement	Ver 5.6 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
535	5.13.3	5.13.3	Wireless Device Risk Mitigations (continued)	2. Are configured for local device authentication (see Section 5.13.8.1).	1	Agency	Agency	Agency
536			"	3. Use advanced authentication or CSO approved compensating controls as per Section 5.13.7.2.1.	1	Agency	Agency	Agency
537			"	4. Encrypt all CJI resident on the device.	1	Agency	Agency	Agency
538			"	5. Erase cached information, to include authenticators (see Section 5.6.2.1) in applications, when session is terminated.	1	Agency	Agency	Agency
539			"	6. Employ personal firewalls or run a Mobile Device Management (MDM) system that facilitates the ability to provide firewall services from the agency level.	1	Agency	Agency	Agency
540			"	7. Employ malicious code protection or run a MDM system that facilitates the ability to provide anti-malware services from the agency level.	1	Agency	Agency	Agency
541	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
542	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
543	~~5.13.4.4~~ ***5.13.4.3***	5.13.4.3	Personal Firewall	A personal firewall **shall** be employed on all devices that have a full-feature operating system (i.e. laptops or tablets with Windows or Linux/Unix operating systems).	1	Agency	Agency	Agency
			"	At a minimum, the personal firewall **shall** perform the following activities:				
544			"	1. Manage program access to the Internet.	1	Agency	Agency	Agency
545			"	2. Block unsolicited requests to connect to the PC.	1	Agency	Agency	Agency
546			"	3. Filter Incoming traffic by IP address or protocol.	1	Agency	Agency	Agency
547			"	4. Filter Incoming traffic by destination ports.	1	Agency	Agency	Agency
548			"	5. Maintain an IP traffic log.	1	Agency	Agency	Agency
549	5.13.5	5.13.5	Incident Response	In addition to the requirements in Section 5.3 Incident Response, agencies **shall** develop additional or enhanced incident reporting and handling procedures to address mobile device operating scenarios.	1	Agency	Agency	Agency
			"	Special reporting procedures for mobile devices **shall** apply in any of the following situations:				
550			"	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				
551			"	2. Total loss of device	1	Agency	Agency	Agency
552			"	3. Device compromise	1	Agency	Agency	Agency
553			"	4. Device loss or compromise outside the United States	1	Agency	Agency	Agency
554	~~5.13.7~~ ***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
555	~~5.13.9.1~~ ***5.13.7.1***	*5.13.7.1*	Local Device Authentication	When mobile devices are authorized for use in accessing CJI, local device authentication **shall** be used to unlock the device for use.	1	Agency	Agency	Agency
556			"	The authenticator used **shall** meet the requirements in section 5.6.2.1 Standard Authenticators.	1	Agency	Agency	Agency
557	***5.13.7.2***	5.13.7.2	Advance Authentication	When accessing CJI from an authorized mobile device, advanced authentication shall be used by the authorized user.	1	Agency	Agency	Agency
558	***5.13.7.2.1***	5.13.7.2.1	Compensating Controls	Before CSOs consider approval of compensating controls, Mobile Device Management (MDM) shall be implemented per Section 5.13.2.	1	Agency	Agency	Agency
			"	The compensating controls shall:				
559			"	1. Meet the intent of the CJIS Security Policy AA requirement	1	Agency	Agency	Agency

	Ver 5.5 Location and New Requirement	Ver 5.6 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
560	***5.13.7.2.1***	5.13.7.2.1	Compensating Controls (continued)	2. Provide a similar level of protection or security as the original AA requirement	1	Agency	Agency	Agency
561			"	3. Not rely upon the existing requirements for AA as compensating controls	1	Agency	Agency	Agency
562			"	At least two of the following examples of AA compensating controls for agency-issued smartphones and tablets with limited feature operating systems shall be implemented to qualify for compensating control consideration:	1	Agency	Agency	Agency
563			"	Possession of the agency-issued smartphone or tablet as an indication it is the authorized user	1	Agency	Agency	Agency
564			"	Implemented password protection on the Mobile Device Mangement application and/or secure container where the authentication application is stored	1	Agency	Agency	Agency
565			"	Enable remote device locking	1	Agency	Agency	Agency
566			"	Enable remote data deletion	1	Agency	Agency	Agency
567			"	Enable automatic data wipe after a predetermined number of failed authentication attempts	1	Agency	Agency	Agency
568			"	Remote device location (GPS) tracking	1	Agency	Agency	Agency
569			"	Require CJIS Security Policy compliant password to access the device	1	Agency	Agency	Agency
570			"	Use of device certificates as per Section 5.13.7.3 Device Certificates	1	Agency	Agency	Agency
	~~5.13.10~~ ***5.13.7.3***	5.13.7.3	Device Certificates	When certificates or cryptographic keys used to authenticate a mobile device are used in lieu of compensating controls for advanced authentication, they **shall** be:				
571			"	1. Protected against being extracted from the device	1	Agency	Agency	Agency
572			"	2. Configured for remote wipe on demand or self-deletion based on a number of unsuccessful login or access attempts	1	Agency	Agency	Agency
573			"	3. Configured to use a secure authenticator (i.e. password, PIN) to unlock the key for use	1	Agency	Agency	Agency