Requirements and Transition Document
FBI CJIS Security Policy Version 5.1
7/13/2012

Requirement Dates Between 2011-2014

Changes to the CJIS Security Policy v5.0 were approved by the Advisory Policy Board (APB) in 2011, and subsequently approved by the Director, FBI, on June 1, 2012. The policy contains current requirements carried over from version 4.5 and 5.0 along with new requirements for agencies to implement.

This document lists every new requirement and its "required by" year from 2011-2014* based on a number of factors including, among other things: cost, threat, technological innovations, and realistic need. Those cases where prior version requirements were assigned a specific "required by" date, i.e. September 30th, 2013, that date has been carried over. CJIS auditors will conduct zero-cycle audits beginning October 1st of the "required by" year. For example, new requirements with a "required by" year of 2012 will fall under the zero-cycle audit beginning October 1st, 2012. Noncriminal Justice Agencies that have 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 will not undergo zero-cycle audits until October 1st, 2013.

The "Summary of Changes" page lists requirements that were added, deleted, or changed from version 5.0 and now reflected in version 5.1. Within the transition document, these modifications are highlighted for ease of location. For continuity, there are columns on the left that reflect policy locations from version 4.5 forward. As new versions are released, these columns will change to indicate current requirement locations in the policy.

Though the dates applied to requirements are spread across several years, the intent is for agencies to start working toward them immediately, where possible, and leverage the requirements document as a tool for financial planning and justification to meet requirements that cannot be met immediately.

Please refer questions or comments about this requirements transition document or version 5.1 of the CJIS Security Policy to your respective Information Security Officer, CJIS Systems Officer, or Compact Officer.

* A requirement with "required by" year without a corresponding month and day is to be read as January 1st of that year.

SUMMARY OF CHANGES

Version 5.1

1. #20 In section 3.2.6, change the words “is to” to the word “shall”
2. #48 and #49 Split paragraph into two (2) separate requirements
3. #50 Section number changed from 4.2.2.1 to 4.2.1
4. #51 Section number changed from 4.2.2.1 to 4.2.1
5. #60 New requirement
6. #61 New requirement
7. #62 New requirement, language change from “is prohibited” to “shall not”
8. #63 New requirement, language change from “must not” to “shall not”
9. #264 Language change from “is prohibited” to “shall not”
10. #379 and #380 Split paragraph into two (2) separate requirements
11. Section 5.9.1.8 Access Records, “2. Signature of the Visitor”, requirement deleted
12. #423 New requirement
13. #431 and #432 Requirement repeated for audit purposes. Please see notes in requirements
14. #465 New requirement
15. #466 Language change in policy, added “and/or” for each sub-bullet
16. #479 New requirement
17. #486 and #487 Split paragraph into two (2) separate requirements

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
	Security Policy Sections 1 - 4 (Introduction, Approach, Roles & Responsibilities, and CJI/PII)				
1	Section 2	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, but shall not detract from the CJIS Security Policy standards.
2	Section 2			"	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, but **shall not** detract from the CJIS Security Policy standards.
3	Section 2			"	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.
4		New (2011) 1.3		"	The policies and procedures **shall** be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.
5	Section 3.1	3.2.1	3.2.1	CJIS Systems Agencies (CSA)	The head of each CSA **shall** appoint a CJIS Systems Officer (CSO).
6		New (2011) 3.2.1		"	Such decisions **shall** be documented and kept current.
7		New (2011) 3.2.2	3.2.2	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.
	Section 3.1 & 3.2	3.2.2		"	The CSO **shall** set, maintain, and enforce the following:
8	Section 3.1 & 3.2	3.2.2(1)	3.2.2(1)	"	1. Standards for the selection, supervision, and separation of personnel who have access to CJI.
9	Section 3.1 & 3.2	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.
10	Section 3.1 & 3.2			"	a. Ensure appropriate use, enforce system discipline, and ensure CJIS Division operating procedures are followed by all users of the respective services and information.
11	Section 3.1 & 3.2			"	b. Ensure state/federal agency compliance with policies approved by the APB and adopted by the FBI.
12	Section 3.1 & 3.2			"	c. Ensure the appointment of the CSA ISO and determine the extent of authority to the CSA ISO.
13		New (2011) 3.2.2(2)		"	d. The CSO, or designee, **shall** ensure that a Terminal Agency Coordinator (TAC) is designated within each agency that has devices accessing CJIS systems.
14	Section 3.1	3.2.2(2)		"	e. Ensure each agency having access to CJI has someone designated as the Local Agency Security Officer (LASO).
15	Section 3.2			"	f. Approve access to FBI CJIS systems.
16	Section 3.2			"	g. Assume ultimate responsibility for managing the security of CJIS systems within their state and/or agency.

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
17	Section 3.2	3.2.2(2)	3.2.2(2)	CJIS Systems Officer (CSO) (continued)	h. Perform other related duties outlined by the user agreements with the FBI CJIS Division.
		New (2011) 3.2.2(3)	3.2.2(3)	"	3. Outsourcing of Criminal Justice Functions
18	Section 3.1.c	3.2.2(3)		"	a. Responsibility for the management of the approved security requirements **shall** remain with the CJA. Security control includes the authority to enforce the standards for the selection, supervision, and separation of personnel who have access to CJI; set and enforce policy governing the operation of computers, circuits, and telecommunications terminals used to process, store, or transmit CJI; and to guarantee the priority service needed by the criminal justice community.
19	Section 3.1.d			"	b. Responsibility for the management control of network security **shall** remain with the CJA. Management control of network security includes the authority to enforce the standards for the selection, supervision, and separation of personnel who have access to CJI; set and enforce policy governing the operation of circuits and network equipment used to transmit CJIS data; and to guarantee the priority service as determined by the criminal justice community.
20	Security Addendum Section 2.01	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.
21	Security Addendum 2.04	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.
	Security Addendum 2.04	3.2.7	3.2.7	"	The AC **shall**:
22	Security Addendum 2.04			"	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.
23	Security Addendum 2.04			"	2. Participate in related meetings and provide input and comments for system improvement.
24	Security Addendum 2.04			"	3. Receive information from the CGA (e.g., system updates) and disseminate it to appropriate Contractor employees.
25	Security Addendum 2.04			"	4. Maintain and update manuals applicable to the effectuation of the agreement, and provide them to the Contractor.
26	Security Addendum 2.04			"	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).

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
27	Security Addendum 2.04	3.2.7	3.2.7	Agency Coordinator (AC) (continued)	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.
28	Security Addendum 2.04			"	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.
29	Security Addendum 2.04			"	8. Where appropriate, ensure compliance by the Contractor with NCIC validation requirements.
30	Security Addendum 2.04			"	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.
31	Security Addendum 2.04			"	10. Any other responsibility for the AC promulgated by the FBI.
	Section 3.3	3.2.8	3.2.8	CJIS System Agency Information Secrurity Officer (CSA ISO)	The CSA ISO **shall**:
32	Section 3.3			"	1. Serve as the security point of contact (POC) to the FBI CJIS Division ISO.
33	Section 3.3			"	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.
34	Section 3.3			"	3. Document and provide assistance for implementing the security-related controls for the Interface Agency and its users.
35	Section 3.3			"	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.
	Section 3.4	3.2.9	3.2.9	Local Agency Security Officer (LASO)	Each LASO **shall**:
36	Section 3.4			"	1. Identify who is using the CSA approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
37	Section 3.4			"	2. Identify and document how the equipment is connected to the state system.
38	Section 3.4			"	3. Ensure that personnel security screening procedures are being followed as stated in this policy.
39	Section 3.4			"	4. Ensure the approved and appropriate security measures are in place and working as expected.
40	Section 3.4			"	5. Support policy compliance and ensure CSA ISO is promptly informed of security incidents.

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
	Section 3.5	3.2.10	3.2.10	FBI CJIS Division Information Security Officer (FBI CJIS ISO)	The FBI CJIS ISO **shall**:
41	Section 3.5			"	1. Maintain the CJIS Security Policy.
42	Section 3.5			"	2. Disseminate the FBI Director approved CJIS Security Policy.
43	Section 3.5			"	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.
44	Section 3.5			"	4. Serve as a point-of-contact (POC) for computer incident notification and distribution of security alerts to the CSOs and ISOs.
45	Section 3.5			"	5. Assist with developing audit compliance guidelines as well as identifying and reconciling security-related issues.
46	Section 3.5			"	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.
47	Section 3.5			"	7. Maintain a current ISO homepage on the Law Enforcement Online (LEO) network and keep the CSOs and ISOs updated on pertinent information via the iso@leo.gov email address.
48		New (2011) 3.2.12	3.2.12	Compact Officer	Pursuant to the National Crime Prevention and Privacy Compact, each party state **shall** appoint a Compact Officer…
49		New (2011) 3.2.12		Compact Officer	...Compact Officer who **shall** ensure that Compact provisions and rules, procedures, and standards established by the Compact Council are complied with in their respective state.
50	Section 8.2.1	4.2.2.1	4.2.1	Proper Access, Use, and Dissemination of CHRI	The III **shall** be accessed only for an authorized purpose.
51	Section 8.2.1			"	Further, CHRI **shall** only be used for an authorized purpose consistent with the purpose for which III was accessed.
52	Section 8.2.1 & 8.2.2	4.2.1	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.
	Section 8.2.1 & 8.2.2	4.2.1	4.2.2	"	The restricted files, which **shall** be protected as CHRI, are as follows:
53	Section 8.2.1 & 8.2.2			"	1. Gang File.
54	Section 8.2.1 & 8.2.2			"	2. Known or Appropriately Suspected Terrorist File.
55	Section 8.2.1 & 8.2.2			"	3. Supervised Release File.
56	Section 8.2.1 & 8.2.2			"	4. Immigration Violator File (formerly the Deported Felon File).
57	Section 8.2.1 & 8.2.2			"	5. National Sex Offender Registry File.
58	Section 8.2.1 & 8.2.2			"	6. Historical Protection Order File of the NCIC.

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
59	Section 8.2.1 & 8.2.2			Proper Access, Use, and Dissemination of NCIC Restricted Files Information (continued)	7. Identity Theft File.
60			New (2012) 4.2.2	"	8. Protective Interest File.
61			New (2012) 4.2.2	"	9. Person With Information [PWI] data in the Missing Person Files.
62	Section 8.2.2.2	4.2.2.2.2	4.2.3.2	For Other Authorized Purposes	Non-restricted files information **shall** not be disseminated commercially.
63			New (2012) 4.2.3.2	"	Agencies **shall not** disseminate restricted files information for purposes other than law enforcement.
64	Section 8.6	4.2.3	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.
65	Section 8.6			"	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.
66	Section 8.3.1	4.2.4.1	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.
67		New (2012) 4.3	4.3	Personally Identifiable Information (PII)	PII **shall** be extracted from CJI for the purpose of official business only.
68		New (2012) 4.3		"	Agencies **shall** develop policies, based on state and local privacy rules, to ensure appropriate controls are applied when handling PII extracted from CJI.

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
	CJIS Security Policy Area 1 - Information Exchange Agreements				
69	Section 7.10(a) & 7.12(a) & 8.5	5.1	5.1	Policy Area 1: Information Exchange Agreements	The information shared through communication mediums **shall** be protected with appropriate security safeguards.
70		New (2012) 5.1.1	5.1.1	Information Exchange	Before exchanging CJI, agencies **shall** put formal agreements in place that specify security controls.
71		New (2012) 5.1.1		"	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.
72		New (2012) 5.1.1		"	Information exchange agreements **shall** be supported by documentation committing both parties to the terms of information exchange.
73		New (2012) 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.
74		New (2012) 5.1.1.1		"	Using the requirements in this policy as a starting point, the procedures **shall** apply to the handling, processing, storing, and communication of CJI.
75	Section 6.2	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.
76	Section 6.2			"	This agreement **shall** include the standards and sanctions governing utilization of CJIS systems.
77	Section 6.2			"	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.
78		New (2012) 5.1.1.2		"	All user agreements with the FBI CJIS Division **shall** be coordinated with the CSA head.
79	Section 6.3	5.1.1.3	5.1.1.3	Criminal Justice Agency User Agreements	Any CJA receiving access to FBI CJIS data **shall** enter into a signed written agreement with the appropriate signatory authority of the CSA providing the access.
80	Section 6.3			"	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.
	Section 6.3			"	These agreements **shall** include:
81	Section 6.3			"	1. Audit.
82	Section 6.3			"	2. Dissemination.
83	Section 6.3			"	3. Hit confirmation.
84	Section 6.3			"	4. Logging.
85	Section 6.3			"	5. Quality Assurance (QA).
86	Section 6.3			"	6. Screening (Pre-Employment).
87	Section 6.3			"	7. Security.
88	Section 6.3			"	8. Timeliness.
89	Section 6.3			"	9. Training.
90	Section 6.3			"	10. Use of the system.
91	Section 6.3			"	11. Validation.

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
92	Section 6.4	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.
93	Section 6.4			"	Access **shall** be permitted when such designation is authorized pursuant to Executive Order, statute, regulation, or inter-agency agreement.
94	Section 6.6	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…
95	Section 6.6			"	...and **shall** be subject to the same extent of audit review as are local user agencies.
96	Security Addendum			"	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.
97	Section 6.7			"	Modifications to the CJIS Security Addendum **shall** be enacted only by the FBI.
98	Section 6.6			"	1. Private contractors designated to perform criminal justice functions for a CJA **shall** be eligible for access to CJI.
99	Section 6.6			"	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.
100	Section 6.6			"	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).
101	Section 6.6			"	2. Private contractors designated to perform criminal justice functions on behalf of a NCJA (government) **shall** be eligible for access to CJI.
102	Section 6.6			"	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.
103	Section 6.6			"	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).
104	Section 2.1.1(b)(4)	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.
105		New (2012) 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.
106	Section 2.1.1(b)(4)	5.1.1.6		"	An NCJA (public) receiving access to FBI CJIS data **shall** enter into a signed written agreement with the appropriate signatory authority of the CSA/SIB providing the access.
107	Section 2.1.1(b)(4)	5.1.1.6		"	A NCJA (private) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions, **shall** be eligible for access to CJI.
108	Section 2.1.1(b)(4)	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.

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
109		New (2012) 5.1.1.6	5.1.1.6	Agency User Agreements (continued)	An NCJA (private) receiving access to FBI CJIS data **shall** enter into a signed written agreement with the appropriate signatory authority of the CSA/SIB providing the access.
110	Section 2.1.1(b)(4)	5.1.1.6		"	All NCJAs accessing CJI **shall** be subject to all pertinent areas of the CJIS Security Policy (see appendix J for supplemental guidance).
111		New (2012) 5.1.1.6		"	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.
112	Section 2.1.1(b)(4)	5.1.1.7	5.1.1.7	Security and Management Control Outsourcing Standard	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.
113	Section 2.1.1(b)(4)	5.1.1.7		"	Access **shall** be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General.
114		New (2011) 5.1.1.7		"	All Channelers accessing CJI **shall** be subject to the terms and conditions described in the Compact Council Security and Management Control Outsourcing Standard.
115	Section 6.4	5.1.1.7		"	Each Channeler that directly accesses CJI **shall** also allow the FBI to conduct periodic penetration testing.
116		New (2011) 5.1.1.7		"	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…
117		New (2011) 5.1.1.7		"	...and **shall** be subject to the same extent of audit review as are local user agencies.
118		New (2012) 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.
119		New (2012) 5.1.2		"	The CJA **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.
120		New (2012) 5.1.2		"	The incident reporting/response process used by the service provider **shall** conform to the incident reporting/response specifications provided in this policy.
121		New (2012) 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.
122		New (2012) 5.1.2.1		"	Evaluation of the risks to the agency **shall** be undertaken based on the criticality of the data, system, and the impact of the change.
123		New (2012) 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.

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
	CJIS Security Policy Area 2 - Security Awareness Training				
124		New (2013) 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.
		New (2013) 5.2.1.1	5.2.1.1	All Personnel	At a minimum, the following topics **shall** be addressed as baseline security awareness training for all authorized personnel with access to CJI:
125				"	1. Rules that describe responsibilities and expected behavior with regard to CJI usage.
126				"	2. Implications of noncompliance.
127				"	3. Incident response (Points of contact; Individual actions).
128				"	4. Media Protection.
129				"	5. Visitor control and physical access to spaces—discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity.
130				"	6. Protect information subject to confidentiality concerns — hardcopy through destruction.
131				"	7. Proper handling and marking of CJI.
132				"	8. Threats, vulnerabilities, and risks associated with handling of CJI.
133				"	9. Dissemination and destruction.
		New (2013) 5.2.1.2	5.2.1.2	Personnel with Physical and Logical Access	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 both physical and logical access to CJI:
134				"	1. Rules that describe responsibilities and expected behavior with regard to information system usage.
135				"	2. Password usage and management—including creation, frequency of changes, and protection.
136				"	3. Protection from viruses, worms, Trojan horses, and other malicious code.
137				"	4. Unknown e-mail/attachments.
138				"	5. Web usage—allowed versus prohibited; monitoring of user activity.
139				"	6. Spam.
140				"	7. Social engineering. (The act of manipulating people to perform actions or divulging confidential information.).
141				"	8. Physical Security—increases in risks to systems and data.
142				"	9. Media Protection.
143				"	10. Handheld device security issues—address both physical and wireless security issues.
144				"	11. Use of encryption and the transmission of sensitive/confidential information over the Internet—address agency policy, procedures, and technical contact for assistance.
145				"	12. Laptop security—address both physical and information security issues.
146				"	13. Personally owned equipment and software—state whether allowed or not (e.g., copyrights).
147				"	14. Access control issues—address least privilege and separation of duties.
148				"	15. Individual accountability—explain what this means in the agency.

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
149		New (2013) 5.2.1.2	5.2.1.2	Personnel with Physical and Logical Access (continued)	16. Use of acknowledgement statements—passwords, access to systems and data, personal use and gain.
150				"	17. Desktop security—discuss use of screensavers, restricting visitors' view of information on screen (preventing/limiting "shoulder surfing"), battery backup devices, allowed access to systems.
151				"	18. Protect information subject to confidentiality concerns—in systems, archived, on backup media, and until destroyed.
152				"	19. Threats, vulnerabilities, and risks associated with accessing CJIS Service systems and services.
		New (2013) 5.2.1.3	5.2.1.3	Personnel with Informatinon Technology Roles	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 Information Technology personnel (system administrators, security administrators, network administrators, etc.):
153				"	1. Protection from viruses, worms, Trojan horses, and other malicious code—scanning, updating definitions.
154				"	2. Data backup and storage—centralized or decentralized approach.
155				"	3. Timely application of system patches—part of configuration management.
156				"	4. Access control measures.
157				"	5. Network infrastructure protection measures.
158	Section 4.3	5.2.2	5.2.2	Security Training Records	Records of individual basic security awareness training and specific information system security training **shall** be:
159					- documented
160					- kept current
161		New (2013) 5.2.2			- maintained by the CSO/SIB/Compact Officer

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
	CJIS Security Policy Area 3 - Incident Response				
162		New (2012) 5.3	5.3	Policy Area 3: Incident Response	Agencies **shall**: (i) establish an operational incident handling capability for agency information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; (ii) track, document, and report incidents to appropriate agency officials and/or authorities.
163		New (2012) 5.3		"	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.
164		New (2012) 5.3.1	5.3.1	Reporting Information Security Events	The agency **shall** promptly report incident information to appropriate authorities.
165		New (2012) 5.3.1		"	Information security events and weaknesses associated with information systems **shall** be communicated in a manner allowing timely corrective action to be taken.
166	Sections 3.3(d) & 5.2.2	5.3.1		"	Formal event reporting and escalation procedures **shall** be in place.
167		New (2012) 5.3.1		"	Wherever feasible, the agency **shall** employ automated mechanisms to assist in the reporting of security incidents.
168		New (2012) 5.3.1		"	All employees, contractors and third party users **shall** be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of agency assets and are required to report any information security events and weaknesses as quickly as possible to the designated point of contact.
	Section 5.2.1	5.3.1.1.1	5.3.1.1.1	FBI CJIS Division Responsibilities	The FBI CJIS Division **shall**:
169	Section 5.2.1			"	1. Manage and maintain the CJIS Division's Computer Security Incident Response Capability (CSIRC).
170	Section 5.2.1			"	2. Serve as a central clearinghouse for all reported intrusion incidents, security alerts, bulletins, and other security-related material.
171	Section 5.2.1			"	3. Ensure additional resources for all incidents affecting FBI CJIS Division controlled systems as needed.
172	Section 5.2.1			"	4. Disseminate prompt advisories of system threats and operating system vulnerabilities to all CSOs and ISOs through the use of the **iso@leo.gov** e-mail account, to include but not limited to: Product Security Bulletins, Virus Bulletins, and Security Clips.
173	Section 5.2.1			"	5. Track all reported incidents and/or trends.
174	Section 5.2.1			"	6. Monitor the resolution of all incidents.
	Section 5.5.2	5.3.1.1.2	5.3.1.1.2	CSA ISO Responsibilities	The CSA ISO **shall**:
175	Section 5.5.2			"	1. Assign individuals in each state, federal, and international law enforcement organization to be the primary point of contact for interfacing with the FBI CJIS Division concerning incident handling and response.
176	Section 5.5.2			"	2. Identify individuals who are responsible for reporting incidents within their area of responsibility.
177	Section 5.5.2			"	3. Collect incident information from those individuals for coordination and sharing among other organizations that may or may not be affected by the incident.

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
178	Section 5.5.2	5.3.1.1.2	5.3.1.1.2	CSA ISO Responsibilities (continued)	4. Develop, implement, and maintain internal incident response procedures and coordinate those procedures with other organizations that may or may not be affected.
179	Section 5.5.2			"	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.
180	Section 5.5.2			"	6. Act as a single POC for their jurisdictional area for requesting incident response assistance.
181	[redacted]	New (2012) 5.3.2	5.3.2	Management of Information Security Incidents	A consistent and effective approach **shall** be applied to the management of information security incidents.
182	Section 5.3 & 5.4	5.3.2		"	Responsibilities and procedures **shall** be in place to handle information security events and weaknesses effectively once they have been reported.
183	[redacted]	New (2012) 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.
184		New (2013) 5.3.2.1		"	Wherever feasible, the agency **shall** employ automated mechanisms to support the incident handling process.
185		New (2012) 5.3.2.2	5.3.2.2	Collection of Evidence	Where a follow-up action against a person or agency after an information security incident involves legal action (either civil or criminal), evidence **shall** be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).
186		New (2012) 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.
187		New (2012) 5.3.4	5.3.4	Incident Monitoring	The agency **shall** track and document information system security incidents on an ongoing basis.
188		New (2012) 5.3.4		"	The CSA ISO **shall** maintain completed security incident reporting forms until the subsequent FBI triennial audit or until legal action (if warranted) is complete (whichever time-frame is greater).

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
	CJIS Security Policy Area 4 - Auditing and Accountability				
189		New (2013) 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.
190		New (2013) 5.4		"	Agencies **shall** carefully assess the inventory of components that compose their information systems to determine which security controls are applicable to the various components.
191	Section 7.14	5.4.1	5.4.1	Auditable Events and Content (Information Systems)	The agency's information system **shall** generate audit records for defined events.
192		New (2013) 5.4.1		"	The agency **shall** specify which information system components carry out auditing activities.
193	Section 7.14	5.4.1		"	The agency's information system **shall** produce, at the application and/or operating system level, audit records containing sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.
194		New (2013) 5.4.1		"	The agency **shall** periodically review and update the list of agency-defined auditable events.
195		New (2013) 5.4.1		"	In the event an agency does not use an automated system, manual recording of activities **shall** still take place.
	Section 7.14	5.4.1.1	5.4.1.1	Events	The following events **shall** be logged:
196	Section 7.14	5.4.1.1		"	1. Successful and unsuccessful system log-on attempts.
197		New (2013) 5.4.1.1		"	2. Successful and unsuccessful attempts to access, create, write, delete or change permission on a user account, file, directory or other system resource.
198	Section 7.14	5.4.1.1		"	3. Successful and unsuccessful attempts to change account passwords.
199		New (2013) 5.4.1.1		"	4. Successful and unsuccessful actions by privileged accounts.
200				"	5. Successful and unsuccessful attempts for users to access, modify, or destroy the audit log file.
		New (2013) 5.4.1.1.1	5.4.1.1.1	Content	The following content **shall** be included with every audited event:
201				"	1. Date and time of the event.
202				"	2. The component of the information system (e.g., software component, hardware component) where the event occurred.
203				"	3. Type of event.
204				"	4. User/subject identity.
205				"	5. Outcome (success or failure) of the event.
206		New (2013) 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.
207		New (2013) 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.
208		New (2013) 5.4.3		"	Audit review/analysis **shall** be conducted at a minimum once a week.
209		New (2013) 5.4.3		"	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.

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
210		New (2013) 5.4.4	5.4.4	Time Stamps	The agency's information system **shall** provide time stamps for use in audit record generation.
211		New (2013) 5.4.4		"	The time stamps **shall** include the date and time values generated by the internal system clocks in the audit records.
212	Section 7.14	5.4.4		"	The agency **shall** synchronize internal information system clocks on an annual basis.
213		New (2013) 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.
214		New (2012) 5.4.6	5.4.6	Audit Record Retention	The agency **shall** retain audit records for at least 365 days.
215		New (2013) 5.4.6		"	Once the minimum retention time period has passed, the agency **shall** continue to retain audit records until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes.
216	Section 8.4	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.
217	Section 8.4	5.4.7		"	The III portion of the log **shall** clearly identify both the operator and the authorized receiving agency.
218	Section 8.4	5.4.7		"	III logs **shall** also clearly identify the requester and the secondary recipient.
219	Section 8.4	5.4.7		"	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.

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
	CJIS Security Policy Area 5 - Access Control				
220		New (2012) 5.5.1	5.5.1	Account Management	The agency **shall** manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts.
221		New (2012) 5.5.1		"	The agency **shall** validate information system accounts at least annually and…
222		New (2012) 5.5.1		"	...and **shall** document the validation process.
223		New (2013) 5.5.1		"	The agency **shall** identify authorized users of the information system and specify access rights/privileges.
		New (2013) 5.5.1		"	The agency **shall** grant access to the information system based on:
224				"	1. Valid need-to-know/need-to-share that is determined by assigned official duties.
225				"	2. Satisfaction of all personnel security criteria.
		New (2013) 5.5.1		"	The agency responsible for account creation **shall** be notified when:
226				"	1. A user's information system usage or need-to-know or need-to-share changes.
227				"	2. A user is terminated or transferred or associated accounts are removed, disabled, or otherwise secured.
228	Section 7.6	5.5.2	5.5.2	Access Enforcement	The information system **shall** enforce assigned authorizations for controlling access to the system and contained information.
229		New (2012) 5.5.2		"	The information system controls **shall** restrict access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel.
230		New (2013) 5.5.2		"	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.
231		New (2013) 5.5.2.1	5.5.2.1	Least Privilege	The agency **shall** approve individual access privileges and…
232		New (2013) 5.5.2.1		"	…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.
233	Section 7.6.3	5.5.2.1		"	The agency **shall** implement least privilege based on specific duties, operations, or information systems as necessary to mitigate risk to CJI.
234		New (2013) 5.5.2.1		"	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.
235		New (2013) 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.
236		New (2013) 5.5.2.2		"	Access controls **shall** be in place and operational for all IT systems to:

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
237		New (2013) 5.5.2.2	5.5.2.2	System Access Control (continued)	1. Prevent multiple concurrent active sessions for one user identification, for those applications accessing CJI, unless the agency grants authority based upon operational business needs. Agencies **shall** document the parameters of the operational business needs for multiple concurrent active sessions.
238		New (2013) 5.5.2.2	5.5.2.2	"	2. Ensure that only authorized personnel can add, change, or remove component devices, dial-up connections, and remove or alter programs.
		New (2013) 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:
239				"	1. Job assignment or function (i.e., the role) of the user seeking access.
240				"	2. Physical location.
241				"	3. Logical location.
242				"	4. Network addresses (e.g., users from sites within a given agency may be permitted greater access than those from outside).
243				"	5. Time-of-day and day-of-week/month restrictions.
		New (2013) 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:
244				"	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.
245				"	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.
246				"	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).
247				"	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.
248	Section 7.6.1	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).
249	Section 7.6.1	5.5.3		"	The system **shall** automatically lock the account/node for a 10 minute time period unless released by an administrator.
250		New (2013) 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.
		New (2013) 5.5.4	5.5.4	"	The system use notification message **shall**, at a minimum, provide the following information:
251				"	1. The user is accessing a restricted information system.
252				"	2. System usage may be monitored, recorded, and subject to audit.

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
253		New (2013) 5.5.4	5.5.4	System Use Notification (continued)	3. Unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties.
254				"	4. Use of the system indicates consent to monitoring and recording.
255		New (2013) 5.5.4	5.5.4	"	The system use notification message **shall** provide appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remain on the screen until the user acknowledges the notification and takes explicit actions to log on to the information system.
256		New (2013) 5.5.4		"	Privacy and security policies **shall** be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.
257	Section 7.6.2, Change 1	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 the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures.
258		New (2013) 5.5.5		"	Users **shall** directly initiate session lock mechanisms to prevent inadvertent viewing when a device is unattended.
259		New (2013) 5.5.6	5.5.6	Remote Access	The agency **shall** authorize, monitor, and control all methods of remote access to the information system.
260		New (2013) 5.5.6		"	The agency **shall** employ automated mechanisms to facilitate the monitoring and control of remote access methods.
261		New (2013) 5.5.6		"	The agency **shall** control all remote accesses through managed access control points.
262		New (2013) 5.5.6		"	The agency may permit remote access for privileged functions only for compelling operational needs but **shall** document the rationale for such access in the security plan for the information system.
263		New (2011) 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.
264		New (2012) 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.
		New (2012) 5.5.7	5.5.7	Wireless Access Restrictions	The agency **shall**:
265				"	(i) establish usage restrictions and implementation guidance for wireless technologies;
266				"	(ii) authorize, monitor, control wireless access to the information system.
		New (2012) 5.5.7.1	5.5.7.1	All 802.11x Wireless Protocols	Agencies **shall**:
267				"	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.
268				"	2. Maintain a complete inventory of all Access Points (APs) and 802.11 wireless devices.
269				"	3. Place APs in secured areas to prevent unauthorized physical access and user manipulation.

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
270		New (2012) 5.5.7.1	5.5.7.1	All 802.11x Wireless Protocols (continued)	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.
271		New (2012) 5.5.7.1	5.5.7.1	"	5. Enable user authentication and encryption mechanisms for the management interface of the AP.
272				"	6. Ensure that all APs have strong administrative passwords and ensure that all passwords are changed in accordance with section 5.6.3.1.
273				"	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.
274				"	8. Change the default service set identifier (SSID) in the APs. Disable the broadcast SSID feature so that the client SSID must match that of the AP. Validate that the SSID character string does not contain any agency identifiable information (division, department, street, etc.) or services.
275				"	9. Enable all security features of the wireless product, including the cryptographic authentication, firewall, and other privacy features.
276				"	10. Ensure that encryption key sizes are at least 128-bits and the default shared keys are replaced by unique keys.
277				"	11. Ensure that the ad hoc mode has been disabled unless the environment is such that the risk has been assessed and is tolerable. Note: some products do not allow disabling this feature; use with caution or use different vendor.
278				"	12. Disable all nonessential management protocols on the APs and disable hypertext transfer protocol (HTTP) when not needed or protect HTTP access with authentication and encryption.
279				"	13. Enable logging (if supported) and review the logs on a recurring basis per local policy. At a minimum logs **shall** be reviewed monthly.
280				"	14. Segregate, virtually (e.g. virtual local area network (VLAN) and ACLs) or physically (e.g. firewalls), the wireless network from the operational wired infrastructure. Limit access between wireless networks and the wired network to only operational needs.
281				"	15. When disposing of access points that will no longer be used by the agency, clear access point configuration to prevent disclosure of network configuration, keys, passwords, etc.
		New (2012) 5.5.7.2	5.5.7.2	Legacy 802.11 Protocols	Agencies **shall** follow the guidelines below regarding wireless implementation and cases where the WEP and WPA security features are used to provide wireless security in conjunction with the CJIS required minimum encryption specifications.
282				"	1. Deploy media access control (MAC) access control lists (ACL); however, MAC ACLs do not represent a strong defense mechanism by themselves because they are transmitted in the clear from WLAN clients to APs so they can be captured easily.
283				"	2. Enable WEP/WPA.

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
284	[redacted]	New (2012) 5.5.7.2	5.5.7.2	Legacy 802.11 Protocols (continued)	3. Ensure the default shared keys are replaced by more secure unique keys.
285				"	4. Enable utilization of key-mapping keys rather than default keys so that sessions are unique when using WEP.
[redacted]		New (2012) 5.5.7.3.1	5.5.7.3.1	Cellular Risk Mitigations	Organizations **shall**, as a minimum, ensure that cellular devices:
286				"	1. Apply available critical patches and upgrades to the operating system.
287				"	2. Are configured for local device authentication.
288				"	3. Use advanced authentication.
289				"	4. Encrypt all CJI resident on the device.
290				"	5. Erase cached information when session is terminated.
291				"	6. Employ personal firewalls.
292				"	7. Employ antivirus software.
293		New (2012) 5.5.7.4	5.5.7.4	Bluetooth	If such services are needed, they **shall** be provided through additional, higher-layer means in addition to the Bluetooth specification and 802.11 standards.
[redacted]		New (2012) 5.5.7.4	5.5.7.4	"	Agencies **shall**:
294				"	1. Provide users with a list of precautionary measures they should take to better protect handheld Bluetooth devices from theft. The organization and its employees should be responsible for its wireless technology components because theft of those components could lead to malicious activities against the organization's information system resource.
295				"	2. Maintain a complete inventory of all Bluetooth-enabled wireless devices and addresses (BD_ADDRs). A complete inventory of Bluetooth-enabled wireless devices can be referenced when conducting an audit that searches for unauthorized use of wireless technologies.
296				"	3. Change the default setting of the Bluetooth device to reflect the organization's security policy. Because default settings are generally not secure, a careful review of those settings should be performed to ensure that they comply with the organization's security policy.
297				"	4. Set Bluetooth devices to the lowest necessary and sufficient power level so that transmissions remain within the secure perimeter of the organization. Setting Bluetooth devices to the lowest necessary and sufficient power level ensures a secure range of access to authorized users. The use of Class 1 devices should be avoided due to their extended range (approximately 100 meters).
298				"	5. Choose personal identification number (PIN) codes that are sufficiently random and long. Avoid static and weak PINs, such as all zeroes. PIN codes should be random so that they cannot be easily reproduced by malicious users. Longer PIN codes are more resistant to brute force attacks. For Bluetooth v2.0 (or earlier) devices, an eight-character alphanumeric PIN **shall** be used.

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
299		New (2012) 5.5.7.4	5.5.7.4	Bluetooth (continued)	6. For v2.1 devices using Secure Simple Pairing, avoid using the “Just Works” model. The “Just Works” model does not provide protection against man-in-the-middle (MITM) attacks. Devices that only support Just Works should not be procured if similarly qualified devices that support one of the association models (i.e. Numeric Comparison, Out of Band, or Passkey Entry) are available.
300		New (2012) 5.5.7.4	5.5.7.4	"	7. Bluetooth devices should be configured by default as, and remain, undiscoverable except as needed for pairing. Bluetooth interfaces should be configured as non-discoverable, which prevents visibility to other Bluetooth devices except when discovery is specifically needed. Also, the default self-identifying or discoverable names provided on Bluetooth devices should be changed to anonymous unidentifiable names.
301				"	8. Invoke link encryption for all Bluetooth connections regardless of how needless encryption may seem (i.e. no Security Mode 1). Link encryption should be used to secure all data transmissions during a Bluetooth connection; otherwise, transmitted data is vulnerable to eavesdropping.
302				"	9. If multi-hop wireless communication is being utilized, ensure that encryption is enabled on every link in the communication chain. Every link should be secured because one unsecured link results in compromising the entire communication chain.
303				"	10. Ensure device mutual authentication is performed for all accesses. Mutual authentication is required to provide verification that all devices on the network are legitimate.
304				"	11. Enable encryption for all broadcast transmission (Encryption Mode 3). Broadcast transmissions secured by link encryption provide a layer of security that protects these transmissions from user interception for malicious purposes.
305				"	12. Configure encryption key sizes to the maximum allowable. Using maximum allowable key sizes provides protection from brute force attacks.
306				"	13. Establish a “minimum key size” for any negotiation process. Establishing minimum key sizes ensures that all keys are long enough to be resistant to brute force attacks. See Section 5.10.1.1.2 for minimum key encryption standards.
307				"	14. Use Security Mode 3 in order to provide link-level security prior to link establishment.
308				"	15. Users do not accept transmissions of any kind from unknown or suspicious devices. These types of transmissions include messages, files, and images. With the increase in the number of Bluetooth enabled devices, it is important that users only establish connections with other trusted devices and only accept content from these trusted devices.

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
	CJIS Security Policy Area 6 - Identification and Authentication				
309		New (2012) 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.
310	Section 7.3.1	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.
311	Section 7.3.1	5.6.1		"	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.
312	Section 7.3.1	5.6.1		"	Agencies **shall** require users to identify themselves uniquely before the user is allowed to perform any actions on the system.
313	Section 7.3.1	5.6.1		"	Agencies **shall** ensure that all user IDs belong to currently authorized users.
314	Section 7.3.1	5.6.1		"	Identification data **shall** be kept current by adding new users and disabling and/or deleting former users.
315	Section 6.1	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.
316	Section 6.1	5.6.1.1		"	The original identifier between the requesting agency and the CSA/SIB/Channeler **shall** be the ORI, and other agency identifiers, such as user identification or personal identifier, an access device mnemonic, or the Internet Protocol (IP) address.
317	Section 6.1	5.6.1.1		"	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.
318	Section 6.1	5.6.1.1		"	Agencies assigned a P (limited access) ORI **shall not** use the full access ORI of another agency to conduct an inquiry transaction.
319		New (2011) 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.
320	Section 7.3.2.2	5.6.2		"	The authentication strategy **shall** be part of the agency's audit for policy compliance.
321	Section 7.3.2.2	5.6.2		"	The FBI CJIS Division **shall** identify and authenticate all individuals who establish direct web-based interactive sessions with FBI CJIS Services.
322		New (2011) 5.6.2		"	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.
323	Section 7.3.3	5.6.2.1	5.6.2.1	Standard Authentication (Password)	Agencies **shall** follow the secure password attributes, below, to authenticate an individual's unique ID.
	Section 7.3.3	5.6.2.1		"	Passwords **shall**:
324	Section 7.3.3			"	1. Be a minimum length of eight (8) characters on all systems.
325	Section 7.3.3			"	2. Not be a dictionary word or proper name.
326	Section 7.3.3			"	3. Not be the same as the Userid.
327	Section 7.3.3			"	4. Expire within a maximum of 90 calendar days.

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
328	Section 7.3.3	5.6.2.1	5.6.2.1	Standard Authentication (Password) (continued)	5. Not be identical to the previous ten (10) passwords.
329	Section 7.3.3			"	6. Not be transmitted in the clear outside the secure location.
330		New (2012) 5.6.2.1		"	7. Not be displayed when entered.
331		New (2012) 5.6.2.2.1	5.6.2.2.1	"	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.
332	Section 7.3.2.2	5.6.3	5.6.3	Identifier and Authenticator Management	The agency **shall** establish identifier and authenticator management processes.
		New (2012) 5.6.3.1	5.6.3.1	Identifier Management	The agency **shall** document and manage user identifiers by:
333				"	1. Uniquely identifying each user.
334				"	2. Verifying the identity of each user.
335				"	3. Receiving authorization to issue a user identifier from an appropriate agency official.
336				"	4. Issuing the user identifier to the intended party.
337				"	5. Disabling the user identifier after a specified period of inactivity.
338				"	6. Archiving user identifiers.
		New (2012) 5.6.3.2	5.6.3.2	Authenticator Management	In order to manage information system authenticators, agencies **shall**:
339				"	1. Define initial authenticator content.
340				"	2. Establish administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators.
341				"	3. Change default authenticators upon information system installation.
342				"	4. Change/refresh authenticators periodically.
343		New (2012) 5.6.3.2		"	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.
		New (2014) 5.6.4	5.6.4	Assertions	Assertion mechanisms used to communicate the results of a remote authentication to other parties **shall** be:
344				"	1. Digitally signed by a trusted entity (e.g., the identity provider).
345				"	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.
346		New (2014) 5.6.4		"	Assertions generated by a verifier **shall** expire after 12 hours and…
347		New (2014) 5.6.4		"	...and **shall not** be accepted thereafter by the relying party.

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
	CJIS Security Policy Area 7 - Configuration Management				
348		New (2011) 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…
349		New (2011) 5.7.1.1		Least Functionality	...and **shall** specifically prohibit and/or restrict the use of specified functions, ports, protocols, and/or services.
350	Section 7.1	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.
	Section 7.1	5.7.1.2		"	The network topological drawing **shall** include the following:
351	Section 7.1			"	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.
352	Section 7.1			"	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.
353	Section 7.1			"	3. "For Official Use Only" (FOUO) markings.
354		New (2012) 5.7.1.2		"	4. The agency name and date (day, month, and year) drawing was created or updated.
355		New (2012) 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.

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
	CJIS Security Policy Area 8 - Media Protection				
356		New (2011) 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.
357		New (2011) 5.8		"	Procedures **shall** be defined for securely handling, transporting and storing media.
358		New (2011) 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.
359		New (2011) 5.8.1		"	The agency **shall** restrict access to electronic and physical media to authorized individuals.
360		New (2013) 5.8.1		"	If physical and personnel restrictions are not feasible then the data **shall** be encrypted per section 5.10.1.2.
361		New (2011) 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.
362		New (2011) 5.8.2.1	5.8.2.1	Electronic Media in Transit	Controls **shall** be in place to protect electronic media containing CJI while in transport (physically moved from one location to another) to help prevent compromise of the data.
363		New (2011) 5.8.2.1		"	Encryption, as defined in section 5.10.1.2 of this policy, is the optimal control during transport; however, if encryption of the data isn't possible then each agency **shall** institute other controls to ensure the security of the data.
364		New (2011) 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.
365	Section 4.6 & 4.7	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.
366	Section 4.6(a)	5.8.3		"	Inoperable electronic media **shall** be destroyed (cut up, shredded, etc.).
367	Section 4.7	5.8.3		"	The agency **shall** maintain written documentation of the steps taken to sanitize or destroy electronic media.
368		New (2011) 5.8.3		"	Agencies **shall** ensure the sanitization or destruction is witnessed or carried out by authorized personnel.
369		New (2011) 5.8.4	5.8.4	Disposal of Physical Media	Physical media **shall** be securely disposed of when no longer required, using formal procedures.
370		New (2011) 5.8.4		"	Formal procedures for the secure disposal or destruction of physical media **shall** minimize the risk of sensitive information compromise by unauthorized individuals.
371	Section 4.6	5.8.4		"	Physical media **shall** be destroyed by shredding or incineration.
372		New (2011) 5.8.4		"	Agencies **shall** ensure the disposal or destruction is witnessed or carried out by authorized personnel.

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
	CJIS Security Policy Area 9 - Physical Protection				
373		New (2011) 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.
374		New (2011) 5.9.1	5.9.1	Physically Secure Location	For interim compliance, and for the sole purpose of meeting the advanced authentication policy, a police vehicle **shall** be considered a physically secure location until September 30th 2013.
375	Section 7.2.2	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.
376	Section 7.2.2	5.9.1.1		"	Security perimeters **shall** be defined, controlled and secured in a manner acceptable to the CSA or SIB.
377		New (2013) 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…
378		New (2013) 5.9.1.2	5.9.1.2	Physical Access Authorizations	...or **shall** issue credentials to authorized personnel.
379	Section 4.4.1	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…
380		New (2011) 5.9.1.3		"	...and **shall** verify individual access authorizations before granting access.
381	Section 4.4.1	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.
382	Section 4.4.1	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…
383	Section 4.4.1	5.9.1.5		Access Control for Display Medium	...and **shall** position information system devices in such a way as to prevent unauthorized individuals from accessing and viewing CJI.
384	Section 4.4.1	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.
385	Section 4.4.1	New (2011) 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).
386	Section 4.4.3	New (2011) 5.9.1.7		"	The agency **shall** escort visitors at all times and monitor visitor activity.
387		New (2012) 5.9.1.8	5.9.1.8	Access Records	The agency **shall** maintain visitor access records to the physically secure location (except for those areas officially designated as publicly accessible) that includes:
388				"	1. Name and agency of the visitor.
				"	2. Signature of the visitor. **NOTE: REMOVED FROM POLICY**
389			5.9.1.8	"	3. Form of identification.
390				"	4. Date of access.
391				"	5. Time of entry and departure.
392				"	6. Purpose of visit.
393				"	7. Name and agency of person visited.
394		New (2012) 5.9.1.8		"	The visitor access records **shall** be maintained for a minimum of one year.

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
395	[redacted]	New (2012) 5.9.1.8	5.9.1.8	Access Records (continued)	Designated officials within the agency **shall** frequently review the visitor access records for accuracy and completeness.
396		New (2013) 5.9.1.9	5.9.1.9	Delivery and Removal	The agency **shall** authorize and control information system-related items entering and exiting the physically secure location.
397		New (2013) 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.
[redacted]		New (2012) 5.9.2		"	The agency **shall**, at a minimum:
398				"	1. Limit access to the controlled area during CJI processing times to only those personnel authorized by the agency to access or view CJI.
399				"	2. Lock the area, room, or storage container when unattended.
400				"	3. Position information system devices and documents containing CJI in such a way as to prevent unauthorized individuals from access and view.
401				"	4. Follow the encryption requirements found in section 5.10.1.1.2 for electronic storage (i.e. data "at rest") of CJI.

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
	CJIS Security Policy Area 10 - Systems and Communications Protection and Information Integrity				
402	Section 7.5	5.10.1	5.10.1	Information Flow Enforcement	The network infrastructure **shall** control the flow of information between interconnected systems.
		New (2013) 5.10.1.1	5.10.1.1	Boundary Protection	The agency **shall**:
403	Section 7	5.10.1.1		"	1. Control access to networks processing CJI.
404		New (2013) 5.10.1.1		"	2. Monitor and control communications at the external boundary of the information system and at key internal boundaries within the system.
405	Section 7.5 & 7.13	5.10.1.1		"	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.
406		New (2013) 5.10.1.1		"	4. Employ tools and techniques to monitor network events, detect attacks, and provide identification of unauthorized use.
407		New (2011) 5.10.1.1		"	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").
408		New (2012) 5.10.1.1		"	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.
409	Section 7.9 & 7.12	5.10.1.2	5.10.1.2	Encryption	1. Encryption **shall** be a minimum of 128 bit.
410	Section 7.9	5.10.1.2		"	2. When CJI is transmitted outside the boundary of the physically secure location, the data **shall** be immediately protected via cryptographic mechanisms (encryption).
411		New (2013) 5.10.1.2		"	3. When CJI is at rest (i.e. stored electronically) outside the boundary of the physically secure location, the data **shall** be protected via cryptographic mechanisms (encryption).
412	Section 7.9 & 7.12	5.10.1.2		"	4. When encryption is employed, the cryptographic module used **shall** be certified to meet FIPS 140-2 standards.
413		New (2013) 5.10.1.2		"	5. For agencies using public key infrastructure technology, the agency **shall** develop and implement a certificate policy and certification practice statement for the issuance of public key certificates used in the information system.
		New (2013) 5.10.1.2		"	Registration to receive a public key certificate **shall**:
414				"	a) Include authorization by a supervisor or a responsible official.
415				"	b) Be accomplished by a secure process that verifies the identity of the certificate holder.
416				"	c) Ensure the certificate is issued to the intended party.
417		New (2013) 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.
		New (2012) 5.10.1.3		"	The CSA/SIB **shall**, in addition:
418				"	1. Monitor inbound and outbound communications for unusual or unauthorized activities.

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
419		New (2012) 5.10.1.3	5.10.1.3	Intrustion Detection Tools and Techniques (continued)	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.
420				"	3. Employ automated tools to support near-real-time analysis of events in support of detecting system-level attacks.
		New (2011) 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:
421				"	1. Establish usage restrictions and implementation guidance for VoIP technologies.
422				"	2. Document, monitor and control the use of VoIP within the agency.
423			New (2013) 5.10.1.4	"	3. Utilize Virtual Local Area Network (VLAN) technology to segment VoIP traffic from data traffic.
424		New (2012) 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.
425		New (2012) 5.10.3.1		"	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).
		New (2012) 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:
426				"	1. Isolate the host from the virtual machine. In other words, virtual machine users cannot access host files, firmware, etc.
427				"	2. Maintain audit logs for all virtual machines and hosts and store the logs outside the hosts' virtual environment.
428				"	3. Virtual Machines that are Internet facing (web servers, portal servers, etc.) **shall** be physically separate from Virtual Machines that process CJI internally.
429				"	4. Device drivers that are "critical" **shall** be contained within a separate guest.
430		New (2011) 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.
431	Section 7.13.1(d)	5.10.4.1		Patch Management	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. **NOTE: Because firewalls were specifically called out in 4.5, audit will continue against firewalls.**
432		New (2011) 5.10.4.1		Patch Management	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. **NOTE: This requirement calls out all network and computing devices including firewalls. Once informational auditing is completed, the firewall specific requirement will be removed.**

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
433		New (2012) 5.10.4.1	5.10.4.1	Patch Management (continued)	Patch requirements discovered during security assessments, continuous monitoring or incident response activities **shall** also be addressed expeditiously.
434		New (2012) 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.
435		New (2012) 5.10.4.2		"	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).
436	Section 7.15	5.10.4.2		"	The agency **shall** employ virus protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses) at critical points throughout the network and on all workstations, servers and mobile computing devices on the network.
437		New (2011) 5.10.4.2		"	The agency **shall** ensure malicious code protection is enabled on all of the aforementioned critical points and information systems and resident scanning is employed.
438		New (2012) 5.10.4.3	5.10.4.3	Spam and Spyware Protection	The agency **shall** implement spam and spyware protection.
		New (2012) 5.10.4.3		"	The agency **shall**:
439				"	1. Employ spam protection mechanisms at critical information system entry points (e.g. firewalls, electronic mail servers, remote-access servers).
440				"	2. Employ spyware protection at workstations, servers or mobile computing devices on the network.
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.
442	Section 7.13.3	5.10.4.4	5.10.4.4	Personal Firewall	A personal firewall **shall** be employed on all devices that are mobile by design (i.e. laptops, handhelds, personal digital assistants, etc.).
	Section 7.13.3(b)	5.10.4.4		"	At a minimum, the personal firewall **shall** perform the following activities:
443	Section 7.13.3(b)			"	1. Manage program access to the Internet.
444	Section 7.13.3(b)			"	2. Block unsolicited requests to connect to the PC.
445	Section 7.13.3(b)			"	3. Filter Incoming traffic by IP address or protocol.
446	Section 7.13.3(b)			"	4. Filter Incoming traffic by destination ports.
447	Section 7.13.3(b)			"	5. Maintain an IP traffic log.
		New (2012) 5.10.4.5	5.10.4.5	Security Alerts and Advisories	The agency **shall**:
448				"	1. Receive information system security alerts/advisories on a regular basis.
449				"	2. Issue alerts/advisories to appropriate personnel.
450				"	3. Document the types of actions to be taken in response to security alerts/advisories.
451				"	4. Take appropriate actions in response.
452				"	5. Employ automated mechanisms to make security alert and advisory information available throughout the agency as appropriate.
453	Section 7.6	5.10.4.6	5.10.4.6	Information Input Restrictions	The agency **shall** restrict the information input to any connection to FBI CJIS services to authorized personnel only.

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
	CJIS Security Policy Area 11 - Formal Audits				
454	Section 9.2	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.
455	Section 9.2	5.11.1.1		"	This audit **shall** include a sample of CJAs and, in coordination with the SIB, the NCJAs.
456		New (2013) 5.11.1.1		"	The FBI CJIS Division **shall** also have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.
457		New (2013) 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.
	Section 9.1	5.11.2	5.11.2	Audits by the CSA	Each CSA **shall**:
458	Section 9.1			"	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.
459		New (2013) 5.11.2		"	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.
460				"	3. Have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.
461	Section 9.4	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.
462	Section 9.4	5.11.3		"	The inspection team **shall** be appointed by the APB and **shall** include at least one representative of the CJIS Division.
463	Section 9.4	5.11.3		"	All results of the inquiry and audit **shall** be reported to the APB with appropriate recommendations.

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
	CJIS Security Policy Area 12 - Personnel Security				
464	Section 4.5.1(a)	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.
465			New (2013) 5.12.1.1	"	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.
466		New (2012) 5.12.1.1	5.12.1.1	"	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.
467	Section 4.5.1(a)	5.12.1.1	5.12.1.1	"	2. All requests for access **shall** be made as specified by the CSO.
468	Section 4.5.1(a)	5.12.1.1		"	All CSO designees **shall** be from an authorized criminal justice agency.
469	Section 4.5.1(b)	5.12.1.1		"	3. If a felony conviction of any kind exists, the hiring authority in the Interface Agency **shall** deny access to CJI.
470	Section 4.5.1(c)	5.12.1.1		"	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.
471	Section 4.5.1(d)	5.12.1.1		"	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.
472	Section 4.5.1(e)	5.12.1.1		"	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.
473		New (2011) 5.12.1.1		"	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.
474	Section 4.5.1(g)	5.12.1.1		"	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.
475	Section 4.5.1(g)	5.12.1.1		"	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.
476	Section 4.5.1(h)	5.12.1.1		"	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.
477	Security Addendum 6.00	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:
478	Security Addendum 6.03	5.12.1.2	5.12.1.2	"	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.

	Ver 4.5 Location	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Topic	Shall Statement
479			New (2013) 5.12.1.2	Personnel Screening for Contractors and Vendors (continued)	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.
480	Security Addendum 6.03(b)	5.12.1.2	5.12.1.2	"	2. If a record of any kind is found, the CGA **shall** be formally notified, and…
481	Security Addendum 6.03(b)	5.12.1.2		"	...and system access **shall** be delayed pending review of the criminal history record information.
482	Security Addendum 6.03(b)	5.12.1.2		"	The CGA **shall** in turn notify the Contractor-appointed Security Officer.
483	Security Addendum 6.03(c)	5.12.1.2		"	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.
484		New (2012) 5.12.1.2		"	4. A Contractor employee found to have a criminal record consisting of felony conviction(s) **shall** be disqualified.
485		New (2012) 5.12.1.2		"	5. Applicants **shall** also be disqualified on the basis of confirmations that arrest warrants are outstanding for such applicants.
486		New (2012) 5.12.1.2	5.12.1.2	"	6. The CGA **shall** maintain a list of personnel who have been authorized access to CJI and…
487		New (2012) 5.12.1.2		"	6. ...and **shall**, upon request, provide a current copy of the access list to the CSO.
488		New (2012) 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.
489	Section 4.2	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.