

	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Ver 5.2 Location and/or New Requirement/Date	Topic	Shall Statement
<b>Security Policy Sections 1 - 4 (Introduction, Approach, Roles &amp; Responsibilities, and CJI/PII)</b>					
1				Relationship to Local Security Policy and Other Policies	The local agency may complement the CJIS Security Policy with a local policy, or the agency may develop their own stand-alone security policy; however, the CJIS Security Policy <b>shall</b> always be the minimum standard and local policy may augment, or increase the standards,...
2	1.3	1.3	1.3	"	...and local policy may augment, or increase the standards, but <b>shall not</b> detract from the CJIS Security Policy standards.
3				"	The agency <b>shall</b> 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 <b>shall</b> be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.
5	3.2.1			CJIS Systems Agencies (CSA)	The head of each CSA <b>shall</b> appoint a CJIS Systems Officer (CSO).
6	New (2011) 3.2.1	3.2.1	3.2.1	"	Such decisions <b>shall</b> be documented and kept current.
7	New (2011) 3.2.2	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 <b>shall not</b> be outsourced.
	3.2.2			"	The CSO <b>shall</b> set, maintain, and enforce the following:
8	3.2.2(1)	3.2.2(1)	3.2.2(1)	"	1. Standards for the selection, supervision, and separation of personnel who have access to CJI.
9				"	2. Policy governing the operation of computers, access devices, circuits, hubs, routers, firewalls, and other components that comprise and support a telecommunications network and related CJIS systems used to process, store, or transmit CJI, guaranteeing the priority, confidentiality, integrity, and availability of service needed by the criminal justice community.
10	3.2.2(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				"	b. Ensure state/federal agency compliance with policies approved by the APB and adopted by the FBI.
12		3.2.2(2)	3.2.2(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, <b>shall</b> ensure that a Terminal Agency Coordinator (TAC) is designated within each agency that has devices accessing CJIS systems.
14				"	e. Ensure each agency having access to CJI has someone designated as the Local Agency Security Officer (LASO).
15	3.2.2(2)			"	f. Approve access to FBI CJIS systems.
16				"	g. Assume ultimate responsibility for managing the security of CJIS systems within their state and/or agency.
17	3.2.2(2)			"	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)	3.2.2(3)	"	3. Outsourcing of Criminal Justice Functions
18	3.2.2(3)	3.2.2(3)	3.2.2(3)	"	a. Responsibility for the management of the approved security requirements <b>shall</b> remain with the CJA.

	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Ver 5.2 Location and/or New Requirement/Date	Topic	Shall Statement
19	3.2.2(3)	3.2.2(3)	3.2.2(3)	CJIS Systems Officer (CSO) (continued)	b. Responsibility for the management control of network security <b>shall</b> remain with the CJA.
20	3.2.6	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 <b>shall</b> appoint an Agency Coordinator.
21	3.2.7	3.2.7	3.2.7	Agency Coordinator (AC)	The AC <b>shall</b> 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.
				"	The AC <b>shall</b> :
22				"	1. Understand the communications, records capabilities, and needs of the Contractor which is accessing federal and state records through or because of its relationship with the CGA.
23				"	2. Participate in related meetings and provide input and comments for system improvement.
24				"	3. Receive information from the CGA (e.g., system updates) and disseminate it to appropriate Contractor employees.
25				"	4. Maintain and update manuals applicable to the effectuation of the agreement, and provide them to the Contractor.
26				"	5. Maintain up-to-date records of Contractor's employees who access the system, including name, date of birth, social security number, date fingerprint card(s) submitted, date security clearance issued, and date initially trained, tested, certified or recertified (if applicable).
27	3.2.7	3.2.7	3.2.7	"	6. Train or ensure the training of Contractor personnel. If Contractor personnel access NCIC, schedule the operators for testing or a certification exam with the CSA staff, or AC staff with permission from the CSA staff. Schedule new operators for the certification exam within six (6) months of assignment. Schedule certified operators for biennial re-certification testing within thirty (30) days prior to the expiration of certification. Schedule operators for other mandated class.
28				"	7. The AC will not permit an untrained/untested or non-certified Contractor employee to access CJI or systems supporting CJI where access to CJI can be gained.
29				"	8. Where appropriate, ensure compliance by the Contractor with NCIC validation requirements.
30				"	9. Provide completed applicant fingerprint cards on each Contractor employee who accesses the system to the CJA (or, where appropriate, CSA) for criminal background investigation prior to such employee accessing the system.
31				"	10. Any other responsibility for the AC promulgated by the FBI.
	3.2.8	3.2.8	3.2.8	CJIS System Agency Information Security Officer (CSA ISO)	The CSA ISO <b>shall</b> :
32				"	1. Serve as the security point of contact (POC) to the FBI CJIS Division ISO.

	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Ver 5.2 Location and/or New Requirement/Date	Topic	Shall Statement
33	3.2.8	3.2.8	3.2.8	CJIS System Agency Information Security Officer (CSA ISO)	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				"	3. Document and provide assistance for implementing the security-related controls for the Interface Agency and its users.
35				"	4. Establish a security incident response and reporting procedure to discover, investigate, document, and report to the CSA, the affected criminal justice agency, and the FBI CJIS Division ISO major incidents that significantly endanger the security or integrity of CJI.
	3.2.9	3.2.9	3.2.9	Local Agency Security Officer (LASO)	Each LASO <b>shall</b> :
36				"	1. Identify who is using the CSA approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
37				"	2. Identify and document how the equipment is connected to the state system.
38				"	3. Ensure that personnel security screening procedures are being followed as stated in this policy.
39				"	4. Ensure the approved and appropriate security measures are in place and working as expected.
40				"	5. Support policy compliance and ensure CSA ISO is promptly informed of security incidents.
	3.2.10	3.2.10	3.2.10	FBI CJIS Division Information Security Officer (FBI CJIS ISO)	The FBI CJIS ISO <b>shall</b> :
41				"	1. Maintain the CJIS Security Policy.
42				"	2. Disseminate the FBI Director approved CJIS Security Policy.
43				"	3. Serve as a liaison with the CSA's ISO and with other personnel across the CJIS community and in this regard provide technical guidance as to the intent and implementation of operational and technical policy issues.
44	3.2.10	3.2.10	3.2.10	FBI CJIS Division Information Security Officer (FBI CJIS ISO) (continued)	4. Serve as a point-of-contact (POC) for computer incident notification and distribution of security alerts to the CSOs and ISOs.
45				"	5. Assist with developing audit compliance guidelines as well as identifying and reconciling security-related issues.
46				"	6. Develop and participate in information security training programs for the CSOs and ISOs, and provide a means by which to acquire feedback to measure the effectiveness and success of such training.
47				"	7. Maintain a security policy resource center (SPRC) on FBI.gov and keep the CSOs and ISOs updated on pertinent information.
48	New (2011) 3.2.12	3.2.12	3.2.12	Compact Officer	Pursuant to the National Crime Prevention and Privacy Compact, each party state <b>shall</b> appoint a Compact Officer...
49	New (2011) 3.2.12				...Compact Officer who <b>shall</b> ensure that Compact provisions and rules, procedures, and standards established by the Compact Council are complied with in their respective state.

	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Ver 5.2 Location and/or New Requirement/Date	Topic	Shall Statement
50	4.2.2.1	4.2.1	4.2.1	Proper Access, Use, and Dissemination of CHRI	The III <b>shall</b> be accessed only for an authorized purpose.
51				"	Further, CHRI <b>shall</b> only be used for an authorized purpose consistent with the purpose for which III was accessed.
52	4.2.1	4.2.2	4.2.2	Proper Access, Use, and Dissemination of NCIC Restricted Files Information	Proper access to, use, and dissemination of data from restricted files <b>shall</b> be consistent with the access, use, and dissemination policies concerning the III described in Title 28, Part 20, CFR, and the NCIC Operating Manual.
	4.2.1	4.2.2	4.2.2	"	The restricted files, which <b>shall</b> be protected as CHRI, are as follows:
53				"	1. Gang File.
54				"	2. Known or Appropriately Suspected Terrorist File.
55				"	3. Supervised Release File.
56				"	4. Immigration Violator File (formerly the Deported Felon File).
57				"	5. National Sex Offender Registry File.
58				"	6. Historical Protection Order File of the NCIC.
59				"	7. Identity Theft File.
60				"	8. Protective Interest File.
61	"	9. Person With Information [PWI] data in the Missing Person Files.			
62	4.2.2.2.2	4.2.3.2	4.2.3.2	For Other Authorized Purposes	Non-restricted files information <b>shall</b> not be disseminated commercially.
63				"	Agencies <b>shall not</b> disseminate restricted files information for purposes other than law enforcement.
64	4.2.3	4.2.4	4.2.4	Storage	When CHRI is stored, agencies <b>shall</b> establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of the information.
65				"	These records <b>shall</b> 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	4.2.4.1	4.2.5.1	4.2.5.1	Justification	In addition to the use of purpose codes and logging information, all users <b>shall</b> 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	4.3	Personally Identifiable Information (PII)	PII <b>shall</b> be extracted from CJI for the purpose of official business only.
68	New (2012) 4.3			"	Agencies <b>shall</b> develop policies, based on state and local privacy rules, to ensure appropriate controls are applied when handling PII extracted from CJI.

	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Ver 5.2 Location and/or New Requirement/Date	Topic	Shall Statement
<b>CJIS Security Policy Area 1 - Information Exchange Agreements</b>					
69	5.1	5.1	5.1	Policy Area 1: Information Exchange Agreements	The information shared through communication mediums <b>shall</b> be protected with appropriate security safeguards.
70	New (2012) 5.1.1	5.1.1	5.1.1	Information Exchange	Before exchanging CJI, agencies <b>shall</b> 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 <b>shall</b> specify the security controls and conditions described in this document.
72	New (2012) 5.1.1			"	Information exchange agreements <b>shall</b> be supported by documentation committing both parties to the terms of information exchange.
73			New 5.1.1	"	<b><i>Law Enforcement and civil agencies shall have a local policy to validate a requestor of CJI as an authorized recipient before disseminating CJI.</i></b>
74	New (2012) 5.1.1.1	5.1.1.1	5.1.1.1	Information Handling	Procedures for handling and storage of information <b>shall</b> be established to protect that information from unauthorized disclosure, alteration or misuse.
75	New (2012) 5.1.1.1			"	Using the requirements in this policy as a starting point, the procedures <b>shall</b> apply to the handling, processing, storing, and communication of CJI.
76	5.1.1.2	5.1.1.2	5.1.1.2	State and Federal Agency User Agreements	Each CSA head or SIB Chief <b>shall</b> 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.
77				"	This agreement <b>shall</b> include the standards and sanctions governing utilization of CJIS systems.
78				"	As coordinated through the particular CSA or SIB Chief, each Interface Agency <b>shall</b> 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.
79				New (2012) 5.1.1.2	"
80	5.1.1.3	5.1.1.3	5.1.1.3	Criminal Justice Agency User Agreements	<b>Any CJA receiving access to FBI CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA providing the access.</b>
81				"	The written agreement <b>shall</b> 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.
				"	These agreements <b>shall</b> include:
82				"	1. Audit.
83				"	2. Dissemination.
84				"	3. Hit confirmation.
85				"	4. Logging.
86				"	5. Quality Assurance (QA).
87				"	6. Screening (Pre-Employment).
88				"	7. Security.
89				"	8. Timeliness.
90	"	9. Training.			
91	"	10. Use of the system.			
92	"	11. Validation.			

	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Ver 5.2 Location and/or New Requirement/Date	Topic	Shall Statement
93	5.1.1.4	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 <b>shall</b> be eligible for access to the CJI.
94				"	Access <b>shall</b> be permitted when such designation is authorized pursuant to Executive Order, statute, regulation, or inter-agency agreement.
95				"	The NCJA <b>shall</b> sign and execute a management control agreement (MCA) with the CJA, which stipulates management control of the criminal justice function remains solely with the CJA.
96	5.1.1.5	5.1.1.5	5.1.1.5	Private Contractor User Agreements and CJIS Security Addendum	Private contractors who perform criminal justice functions <b>shall</b> meet the same training and certification criteria required by governmental agencies performing a similar function, and...
97				"	...and <b>shall</b> be subject to the same extent of audit review as are local user agencies.
98				"	All private contractors who perform criminal justice functions <b>shall</b> acknowledge, via signing of the Security Addendum Certification page, and abide by all aspects of the CJIS Security Addendum.
99				"	Modifications to the CJIS Security Addendum <b>shall</b> be enacted only by the FBI.
100				"	1. Private contractors designated to perform criminal justice functions for a CJA <b>shall</b> be eligible for access to CJI.
101				"	Access <b>shall</b> be permitted pursuant to an agreement which specifically identifies the agency's purpose and scope of providing services for the administration of criminal justice.
102				"	The agreement between the CJA and the private contractor <b>shall</b> 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).
103				"	2. Private contractors designated to perform criminal justice functions on behalf of a NCJA (government) <b>shall</b> be eligible for access to CJI.
104				"	Access <b>shall</b> be permitted pursuant to an agreement which specifically identifies the agency's purpose and scope of providing services for the administration of criminal justice.
105	"	The agreement between the NCJA and the private contractor <b>shall</b> 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).			
106	5.1.1.6	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, <b>shall</b> be eligible for access to CJI.
107	New (2012) 5.1.1.6			"	Access <b>shall</b> be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General.
108	5.1.1.6			"	A NCJA (public) receiving access to FBI <u>CJ/</u> <b>shall</b> enter into a signed written agreement with the appropriate signatory authority of the CSA/SIB providing the access.
109	5.1.1.6	5.1.1.6	5.1.1.6	"	A NCJA (private) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions, <b>shall</b> be eligible for access to CJI.

	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Ver 5.2 Location and/or New Requirement/Date	Topic	Shall Statement
110	5.1.1.6	5.1.1.6	5.1.1.6	Agency User Agreements (continued)	Access <b>shall</b> be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General.
111	New (2012) 5.1.1.6			"	A NCJA (private) receiving access to FBI <u>CJI</u> <b>shall</b> enter into a signed written agreement with the appropriate signatory authority of the <u>CSA, SIB, or authorized agency</u> providing the access.
112	5.1.1.6			"	All NCJAs accessing CJI <b>shall</b> be subject to all pertinent areas of the CJIS Security Policy (see appendix J for supplemental guidance).
113	New (2012) 5.1.1.6			"	Each NCJA that directly accesses FBI CJI <b>shall</b> 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.
114	5.1.1.7	5.1.1.7	5.1.1.7	<u>Outsourcing Standards for Channelers</u>	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 <b>shall</b> be eligible for access to CJI.
115	5.1.1.7			"	Access <b>shall</b> be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General.
116	New (2011) 5.1.1.7			"	All Channelers accessing CJI <b>shall</b> be subject to the terms and conditions described in the Compact Council Security and Management Control Outsourcing Standard.
117	5.1.1.7			"	Each Channeler that directly accesses CJI <b>shall</b> also allow the FBI to conduct periodic penetration testing.
118	New (2011) 5.1.1.7			"	Channelers leveraging CJI to perform civil functions on behalf of an Authorized Recipient <b>shall</b> meet the same training and certification criteria required by governmental agencies performing a similar function...
119	New (2011) 5.1.1.7			"	...and <b>shall</b> be subject to the same extent of audit review as are local user agencies.
120				<u>Outsourcing Standards for Non-Channelers</u>	<u>Contractors designated to perform noncriminal justice ancillary functions on behalf of a NCJA (public) or NCJA (private) for noncriminal justice functions shall be eligible for access to CJI.</u>
121				"	<u>Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General.</u>
122			New 5.1.1.8	"	<u>All contractors accessing CJI shall be subject to the terms and conditions described in the Compact Council Outsourcing Standard for Non-Channelers.</u>
123				"	<u>Contractors leveraging CJI to perform civil functions on behalf of an Authorized Recipient shall meet the same training and certification criteria required by governmental agencies performing a similar function, and...</u>
124				"	<u>...and shall be subject to the same extent of audit review as are local user agencies.</u>
125	New (2012) 5.1.2	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 <b>shall</b> be regularly monitored and reviewed.
126	New (2012) 5.1.2			"	The CJA, <u>authorized agency, or FBI</u> <b>shall</b> 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.

	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Ver 5.2 Location and/or New Requirement/Date	Topic	Shall Statement
127	New (2012) 5.1.2	5.1.2	5.1.2	Monitoring, Review, and Delivery of Services (continued)	The incident reporting/response process used by the service provider <b>shall</b> conform to the incident reporting/response specifications provided in this policy.
128	New (2012) 5.1.2.1	5.1.2.1	5.1.2.1	Managing Changes to Service Providers	<b>Any changes to services provided by a service provider shall be managed by the CJA, authorized agency, or FBI.</b>
129	New (2012) 5.1.2.1			"	Evaluation of the risks to the agency <b>shall</b> be undertaken based on the criticality of the data, system, and the impact of the change.
130	New (2012) 5.1.3	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 <b>shall</b> log such dissemination.
131			New 5.1.4	<u>Secondary Dissemination of Non-CHRI CJI</u>	<u>Dissemination shall conform to the local policy validating the requestor of the CJI as an employee or contractor of a law enforcement agency or civil agency requiring the CJI to perform their mission or a member of the public receiving CJI via authorized dissemination.</u>

	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Ver 5.2 Location and/or New Requirement/Date	Topic	Shall Statement
<b>CJIS Security Policy Area 2 - Security Awareness Training</b>					
132	New (2013) 5.2	5.2	5.2	Policy Area 2: Security Awareness Training	Basic security awareness training <b>shall</b> be required within six months of initial assignment and biennially thereafter, for all personnel who have access to CJJ.
	New (2013) 5.2.1.1	5.2.1.1	5.2.1.1	All Personnel	At a minimum, the following topics <b>shall</b> be addressed as baseline security awareness training for all authorized personnel with access to CJJ:
133				"	1. Rules that describe responsibilities and expected behavior with regard to CJJ usage.
134				"	2. Implications of noncompliance.
135				"	3. Incident response (Points of contact; Individual actions).
136				"	4. Media Protection.
137				"	5. Visitor control and physical access to spaces—discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity.
138				"	6. Protect information subject to confidentiality concerns — hardcopy through destruction.
139				"	7. Proper handling and marking of CJJ.
140				"	8. Threats, vulnerabilities, and risks associated with handling of CJJ.
141				New (2013) 5.2.1.2	5.2.1.2
142	New (2013) 5.2.1.1	5.2.1.1	5.2.1.1	"	<u>10. Dissemination and destruction.</u>
	New (2013) 5.2.1.2	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, <b>shall</b> be addressed as baseline security awareness training for all authorized personnel with both physical and logical access to CJJ:
143				"	1. Rules that describe responsibilities and expected behavior with regard to information system usage.
144				"	2. Password usage and management—including creation, frequency of changes, and protection.
145				"	3. Protection from viruses, worms, Trojan horses, and other malicious code.
146				"	4. Unknown e-mail/attachments.
147				"	5. Web usage—allowed versus prohibited; monitoring of user activity.
148				"	6. Spam.
149				"	<u>7. Physical Security—increases in risks to systems and data.</u>
150				"	<u>8. Handheld device security issues—address both physical and wireless security issues.</u>
151				"	<u>9. Use of encryption and the transmission of sensitive/confidential information over the Internet—address agency policy, procedures, and technical contact for assistance.</u>
152				"	<u>10. Laptop security—address both physical and information security issues.</u>
153				"	<u>11. Personally owned equipment and software—state whether allowed or not (e.g., copyrights).</u>
154				"	<u>12. Access control issues—address least privilege and separation of duties.</u>
155	"	<u>13. Individual accountability—explain what this means in the agency.</u>			

	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Ver 5.2 Location and/or New Requirement/Date	Topic	Shall Statement
156	New (2013) 5.2.1.2	5.2.1.2	5.2.1.2	Personnel with Physical and Logical Access (continued)	14. Use of acknowledgement statements—passwords, access to systems and data, personal use and gain.
157				"	15. Desktop security—discuss use of screensavers, restricting visitors' view of information on screen (preventing/limiting "shoulder surfing"), battery backup devices, allowed access to systems.
158				"	16. Protect information subject to confidentiality concerns—in systems, archived, on backup media, and until destroyed.
159				"	17. Threats, vulnerabilities, and risks associated with accessing CJIS Service systems and services.
	New (2013) 5.2.1.3	5.2.1.3	5.2.1.3	Personnel with Information Technology Roles	In addition to 5.2.1.1 and 5.2.1.2 above, the following topics at a minimum <b>shall</b> be addressed as baseline security awareness training for all Information Technology personnel (system administrators, security administrators, network administrators, etc.):
160				"	1. Protection from viruses, worms, Trojan horses, and other malicious code—scanning, updating definitions.
161				"	2. Data backup and storage—centralized or decentralized approach.
162				"	3. Timely application of system patches—part of configuration management.
163				"	4. Access control measures.
164	"	5. Network infrastructure protection measures.			
	5.2.2	5.2.2	5.2.2	Security Training Records	Records of individual basic security awareness training and specific information system security training <b>shall</b> be:
165					- documented
166					- kept current
167	New (2013) 5.2.2				- maintained by the CSO/SIB/Compact Officer

	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Ver 5.2 Location and/or New Requirement/Date	Topic	Shall Statement
<b>CJIS Security Policy Area 3 - Incident Response</b>					
168	New (2012) 5.3	5.3	5.3	Policy Area 3: Incident Response	Agencies <b>shall</b> : (i) establish an operational incident handling capability for agency information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities;...
169	New (2012) 5.3			"	...(ii) track, document, and report incidents to appropriate agency officials and/or authorities.
170	New (2012) 5.3			"	ISOs have been identified as the POC on security-related issues for their respective agencies and <b>shall</b> ensure LASOs institute the CSA incident response reporting procedures at the local level.
171	New (2012)	5.3.1	5.3.1	Reporting Information Security	The agency <b>shall</b> promptly report incident information to appropriate authorities.
172	New (2012) 5.3.1			"	Information security events and weaknesses associated with information systems <b>shall</b> be communicated in a manner allowing timely corrective action to be taken.
173	5.3.1			"	Formal event reporting and escalation procedures <b>shall</b> be in place.
174	New (2012) 5.3.1			"	Wherever feasible, the agency <b>shall</b> employ automated mechanisms to assist in the reporting of security incidents.
175	New (2012) 5.3.1			"	All employees, contractors and third party users <b>shall</b> 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.
176	5.3.1.1.1	5.3.1.1.1	5.3.1.1.1	FBI CJIS Division Responsibilities	The FBI CJIS Division <b>shall</b> :
177				"	1. Manage and maintain the CJIS Division's Computer Security Incident Response Capability (CSIRC).
178				"	2. Serve as a central clearinghouse for all reported intrusion incidents, security alerts, bulletins, and other security-related material.
179				"	3. Ensure additional resources for all incidents affecting FBI CJIS Division controlled systems as needed.
180				"	4. Disseminate prompt advisories of system threats and operating system vulnerabilities <i>via the security policy resource center on FBI.gov</i> , to include but not limited to: Product Security Bulletins, Virus Bulletins, and Security Clips.
181				"	5. Track all reported incidents and/or trends.
182	5.3.1.1.2	5.3.1.1.2	5.3.1.1.2	CSA ISO Responsibilities	The CSA ISO <b>shall</b> :
183				"	1. Assign individuals in each state, federal, and international law enforcement organization to be the primary point of contact for interfacing with the FBI CJIS Division concerning incident handling and response.
184				"	2. Identify individuals who are responsible for reporting incidents within their area of responsibility.
					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 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Ver 5.2 Location and/or New Requirement/Date	Topic	Shall Statement
185	5.3.1.1.2	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.
186				"	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.
187				"	6. Act as a single POC for their jurisdictional area for requesting incident response assistance.
188	New (2012) 5.3.2	5.3.2	5.3.2	Management of Information Security Incidents	A consistent and effective approach <b>shall</b> be applied to the management of information security incidents.
189	5.3.2			"	Responsibilities and procedures <b>shall</b> be in place to handle information security events and weaknesses effectively once they have been reported.
190	New (2012) 5.3.2.1	5.3.2.1	5.3.2.1	Incident Handling	The agency <b>shall</b> implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.
191	New (2013) 5.3.2.1			"	Wherever feasible, the agency <b>shall</b> employ automated mechanisms to support the incident handling process.
192	New (2012) 5.3.2.2	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 <b>shall</b> be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).
193	New (2012) 5.3.3	5.3.3	5.3.3	Incident Response Training	The agency <b>shall</b> ensure general incident response roles responsibilities are included as part of required security awareness training.
194	New (2012) 5.3.4	5.3.4	5.3.4	Incident Monitoring	The agency <b>shall</b> track and document information system security incidents on an ongoing basis.
195	New (2012) 5.3.4			"	The CSA ISO <b>shall</b> 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 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Ver 5.2 Location and/or New Requirement/Date	Topic	Shall Statement		
<b>CJIS Security Policy Area 4 - Auditing and Accountability</b>							
196	New (2013) 5.4	5.4	5.4	Policy Area 4: Auditing and Accountability	Agencies <b>shall</b> implement audit and accountability controls to increase the probability of authorized users conforming to a prescribed pattern of behavior.		
197	New (2013) 5.4			"	Agencies <b>shall</b> carefully assess the inventory of components that compose their information systems to determine which security controls are applicable to the various components.		
198	5.4.1	5.4.1	5.4.1	Auditable Events and Content (Information Systems)	The agency's information system <b>shall</b> generate audit records for defined events.		
199	New (2013) 5.4.1			"	The agency <b>shall</b> specify which information system components carry out auditing activities.		
200	5.4.1			"	The agency's information system <b>shall</b> 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.		
201	New (2013) 5.4.1			"	The agency <b>shall</b> periodically review and update the list of agency-defined auditable events.		
202	New (2013) 5.4.1			"	In the event an agency does not use an automated system, manual recording of activities <b>shall</b> still take place.		
	5.4.1.1			5.4.1.1	5.4.1.1	Events	The following events <b>shall</b> be logged:
203	5.4.1.1					"	1. Successful and unsuccessful system log-on attempts.
204	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.				
205	5.4.1.1	"	3. Successful and unsuccessful attempts to change account passwords.				
206		"	4. Successful and unsuccessful actions by privileged accounts.				
207	New (2013) 5.4.1.1	"	5. Successful and unsuccessful attempts for users to access, modify, or destroy the audit log file.				
		5.4.1.1.1	5.4.1.1.1			Content	The following content <b>shall</b> be included with every audited event:
208				"	1. Date and time of the event.		
209	New (2013) 5.4.1.1.1			"	2. The component of the information system (e.g., software component, hardware component) where the event occurred.		
210				"	3. Type of event.		
211				"	4. User/subject identity.		
212		"	5. Outcome (success or failure) of the event.				
213	New (2013) 5.4.2	5.4.2	5.4.2	Response to Audit Processing Failures	The agency's information system <b>shall</b> provide alerts to appropriate agency officials in the event of an audit processing failure.		
214	New (2013) 5.4.3	5.4.3	5.4.3	Audit Monitoring, Analysis, and Reporting	The responsible management official <b>shall</b> 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.		
215	New (2013) 5.4.3			"	Audit review/analysis <b>shall</b> be conducted at a minimum once a week.		

	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Ver 5.2 Location and/or New Requirement/Date	Topic	Shall Statement
216	New (2013) 5.4.3	5.4.3	5.4.3	Audit Monitoring, Analysis, and Reporting (continued)	The agency <b>shall</b> 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.
217	New (2013) 5.4.4	5.4.4	5.4.4	Time Stamps	The agency's information system <b>shall</b> provide time stamps for use in audit record generation.
218	New (2013) 5.4.4			"	The time stamps <b>shall</b> include the date and time values generated by the internal system clocks in the audit records.
219	5.4.4			"	The agency <b>shall</b> synchronize internal information system clocks on an annual basis.
220	New (2013) 5.4.5	5.4.5	5.4.5	Protection of Audit Information	The agency's information system <b>shall</b> protect audit information and audit tools from modification, deletion and unauthorized access.
221	New (2012) 5.4.6	5.4.6	5.4.6	Audit Record Retention	The agency <b>shall</b> retain audit records for at least <u>one (1) year</u> .
222	New (2013) 5.4.6			"	Once the minimum retention time period has passed, the agency <b>shall</b> continue to retain audit records until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes.
223	5.4.7	5.4.7	5.4.7	Logging NCIC and III Transactions	A log <b>shall</b> be maintained for a minimum of one (1) year on all NCIC and III transactions.
224	5.4.7			"	The III portion of the log <b>shall</b> clearly identify both the operator and the authorized receiving agency.
225	5.4.7			"	III logs <b>shall</b> also clearly identify the requester and the secondary recipient.
226	5.4.7			"	The identification on the log <b>shall</b> take the form of a unique identifier that <b>shall</b> remain unique to the individual requester and to the secondary recipient throughout the minimum one year retention period.

	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Ver 5.2 Location and/or New Requirement/Date	Topic	Shall Statement
<b>CJIS Security Policy Area 5 - Access Control</b>					
227	New (2012) 5.5.1	5.5.1	5.5.1	Account Management	The agency <b>shall</b> manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts.
228	New (2012) 5.5.1			"	The agency <b>shall</b> validate information system accounts at least annually and...
229	New (2012) 5.5.1			"	...and <b>shall</b> document the validation process.
230	New (2013) 5.5.1			"	The agency <b>shall</b> identify authorized users of the information system and specify access rights/privileges.
				"	The agency <b>shall</b> grant access to the information system based on:
231	New (2013) 5.5.1			"	1. Valid need-to-know/need-to-share that is determined by assigned official duties.
232				"	2. Satisfaction of all personnel security criteria.
				"	The agency responsible for account creation <b>shall</b> be notified when:
233	New (2013) 5.5.1			"	1. A user's information system usage or need-to-know or need-to-share changes.
234				"	2. A user is terminated or transferred or associated accounts are removed, disabled, or otherwise secured.
235	5.5.2	5.5.2	5.5.2	Access Enforcement	The information system <b>shall</b> enforce assigned authorizations for controlling access to the system and contained information.
236	New (2012) 5.5.2			"	The information system controls <b>shall</b> restrict access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel.
237	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) <b>shall</b> 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.
238	New (2013) 5.5.2.1	5.5.2.1	5.5.2.1	Least Privilege	The agency <b>shall</b> approve individual access privileges and...
239	New (2013) 5.5.2.1			"	...and <b>shall</b> enforce physical and logical access restrictions associated with changes to the information system; and generate, retain, and review records reflecting all such changes.
240	New (2013) 5.5.2.1			"	The agency <b>shall</b> enforce the most restrictive set of rights/privileges or access needed by users for the performance of specified tasks.
241	5.5.2.1			"	The agency <b>shall</b> implement least privilege based on specific duties, operations, or information systems as necessary to mitigate risk to CJI.
242	New (2013) 5.5.2.1			"	Logs of access privilege changes <b>shall</b> be maintained for a minimum of one year or at least equal to the agency's record retention policy – whichever is greater.
243	New (2013) 5.5.2.2	5.5.2.2	5.5.2.2	System Access Control	Access control mechanisms to enable access to CJI <b>shall</b> be restricted by object (e.g., data set, volumes, files, records) including the ability to read, write, or delete the objects.

	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Ver 5.2 Location and/or New Requirement/Date	Topic	Shall Statement
	New (2013) 5.5.2.2	5.5.2.2	5.5.2.2	System Access Control (continued)	Access controls <b>shall</b> be in place and operational for all IT systems to:
244	New (2013) 5.5.2.2	5.5.2.2		"	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.
245	New (2013) 5.5.2.2	5.5.2.2		"	(1. continued) Agencies <b>shall</b> document the parameters of the operational business needs for multiple concurrent active sessions.
246	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	5.5.2.3	Access Control Criteria	Agencies <b>shall</b> control access to CJI based on one or more of the following:
247				"	1. Job assignment or function (i.e., the role) of the user seeking access.
248				"	2. Physical location.
249				"	3. Logical location.
250				"	4. Network addresses (e.g., users from sites within a given agency may be permitted greater access than those from outside).
251				"	5. Time-of-day and day-of-week/month restrictions.
	New (2013) 5.5.2.4	5.5.2.4	5.5.2.4	Access Control Mechanisms	When setting up access controls, agencies <b>shall</b> use one or more of the following mechanisms:
252				"	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.
253				"	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.
254				"	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).
255				"	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.
256	5.5.3	5.5.3	5.5.3	Unsuccessful Login Attempts	Where technically feasible, the system <b>shall</b> 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).
257	5.5.3			"	The system <b>shall</b> automatically lock the account/node for a 10 minute time period unless released by an administrator.
258	New (2013) 5.5.4	5.5.4	5.5.4	System Use Notification	The information system <b>shall</b> display an approved system use notification message, before granting access, informing potential users of various usages and monitoring rules.
	New (2013) 5.5.4			"	The system use notification message <b>shall</b> , at a minimum, provide the following information:

	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Ver 5.2 Location and/or New Requirement/Date	Topic	Shall Statement
259	New (2013) 5.5.4	5.5.4	5.5.4	System Use Notification (continued)	1. The user is accessing a restricted information system.
260				"	2. System usage may be monitored, recorded, and subject to audit.
261				"	3. Unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties.
262				"	4. Use of the system indicates consent to monitoring and recording.
263	New (2013) 5.5.4	5.5.4	5.5.4	"	The system use notification message <b>shall</b> provide appropriate privacy and security notices (based on associated privacy and security policies or summaries) and...
264	New (2013) 5.5.4			"	...and remain on the screen until the user acknowledges the notification and takes explicit actions to log on to the information system.
265	New (2013) 5.5.4			"	Privacy and security policies <b>shall</b> be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.
266	5.5.5	5.5.5	5.5.5	Session Lock	The information system <b>shall</b> prevent further access to the system by initiating a session lock after a maximum of 30 minutes of inactivity, and...
267	5.5.5			"	...and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures.
268	New (2013) 5.5.5			"	Users <b>shall</b> directly initiate session lock mechanisms to prevent inadvertent viewing when a device is unattended.
269	New (2013) 5.5.6	5.5.6	5.5.6	Remote Access	The agency <b>shall</b> authorize, monitor, and control all methods of remote access to the information system.
270	New (2013) 5.5.6			"	The agency <b>shall</b> employ automated mechanisms to facilitate the monitoring and control of remote access methods.
271	New (2013) 5.5.6			"	The agency <b>shall</b> control all remote accesses through managed access control points.
272	New (2013) 5.5.6			"	The agency may permit remote access for privileged functions only for compelling operational needs but <b>shall</b> document the rationale for such access in the security plan for the information system.
273	New (2011) 5.5.6.1	5.5.6.1	5.5.6.1	Personally Owned Information Systems	A personally owned information system <b>shall not</b> be authorized to access, process, store or transmit CJJ unless the agency has established and documented the specific terms and conditions for personally owned information system usage.
274			New 5.5.6.1	<u>Personally Owned Information Systems</u>	<u>When Bring Your Own Devices (BYOD) are authorized, they shall be controlled using the requirements in Section 5.5.7.3 Cellular.</u>
275	New (2012) 5.5.6.2	5.5.6.2	5.5.6.2	Publicly Accessible Computers	Publicly accessible computers <b>shall not</b> be used to access, process, store or transmit CJJ. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.
				Wireless Access Restrictions	The agency <b>shall</b> :
276	New (2012) 5.5.7	5.5.7	5.5.7	"	(i) establish usage restrictions and implementation guidance for wireless technologies;
277				"	(ii) authorize, monitor, control wireless access to the information system.
				All 802.11x Wireless Protocols	Agencies <b>shall</b> :
278	New (2012) 5.5.7.1	5.5.7.1	5.5.7.1	"	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.

	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Ver 5.2 Location and/or New Requirement/Date	Topic	Shall Statement
279	New (2012) 5.5.7.1	5.5.7.1	5.5.7.1	All 802.11x Wireless Protocols (continued)	2. Maintain a complete inventory of all Access Points (APs) and 802.11 wireless devices.
280				"	3. Place APs in secured areas to prevent unauthorized physical access and user manipulation.
281				"	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.
282				"	5. Enable user authentication and encryption mechanisms for the management interface of the AP.
283				"	6. Ensure that all APs have strong administrative passwords and ensure that all passwords are changed in accordance with section 5.6.3.1.
284				"	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.
285				"	8. Change the default service set identifier (SSID) in the APs.
286				"	Disable the broadcast SSID feature so that the client SSID must match that of the AP.
287				"	Validate that the SSID character string does not contain any agency identifiable information (division, department, street, etc.) or services.
288				"	9. Enable all security features of the wireless product, including the cryptographic authentication, firewall, and other privacy features.
289				"	10. Ensure that encryption key sizes are at least 128-bits and the default shared keys are replaced by unique keys.
290				"	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.
291				"	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.
292				"	13. Enable logging (if supported) and...
293				"	...and review the logs on a recurring basis per local policy.
294				"	At a minimum logs <b>shall</b> be reviewed monthly.
295				"	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.
296				"	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	5.5.7.2	Legacy 802.11 Protocols	Agencies <b>shall</b> 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.

	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Ver 5.2 Location and/or New Requirement/Date	Topic	Shall Statement
297	New (2012) 5.5.7.2	5.5.7.2	5.5.7.2	Legacy 802.11 Protocols (continued)	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.
298				"	2. Enable WEP/WPA.
299				"	3. Ensure the default shared keys are replaced by more secure unique keys.
300				"	4. Enable utilization of key-mapping keys rather than default keys so that sessions are unique when using WEP.
301	New (2012) 5.5.7.3.1	5.5.7.3.1	5.5.7.3.1	Cellular Risk Mitigations	Organizations <b>shall</b> , as a minimum, ensure that cellular devices:
302				"	1. Apply available critical patches and upgrades to the operating system <u>as soon as they become available for the device and after necessary testing as described in Section 5.10.4.1</u> .
303				"	2. Are configured for local device authentication.
304				"	3. Use advanced authentication.
305				"	4. Encrypt all CJI resident on the device.
306				"	5. Erase cached information when session is terminated.
307				"	6. Employ personal firewalls <u>or run a Mobile Device Management system that facilitates the ability to provide firewall services from the agency level</u> .
308	New 5.5.7.3.3	5.5.7.3.3	5.5.7.3.3	<u>Mobile Device Management (MDM)</u>	<u>Devices that have been rooted, jailbroken, or have had any unauthorized changes made to them shall not be used to process, store, or transmit CJI at any time.</u>
309				"	<u>In addition to the security controls described in this policy, agencies shall implement the following controls when allowing CJI access from cell/smart phones and tablet devices.</u>
310				"	1. <u>CJI is only transferred between CJI authorized applications and storage areas of the device.</u>
311				"	2. <u>MDM with centralized administration capable of at least:</u>
312				"	<u>i. Remote locking of the device</u>
313				"	<u>ii. Remote wiping of the device</u>
314				"	<u>iii. Setting and locking device configuration</u>
315	"	<u>iv. Detection of "rooted" and/or "jailbroken" devices</u>			
316	New (2012) 5.5.7.4	5.5.7.4	5.5.7.4	Bluetooth	If such services are needed, they <b>shall</b> be provided through additional, higher-layer means in addition to the Bluetooth specification and 802.11 standards.
317				"	Agencies <b>shall</b> :
				"	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.

	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Ver 5.2 Location and/or New Requirement/Date	Topic	Shall Statement
318	New (2012) 5.5.7.4	5.5.7.4	5.5.7.4	Bluetooth (continued)	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.
319				"	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.
320				"	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).
321				"	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 <b>shall</b> be used.
322				"	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.
323				"	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.
324				"	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.
325				"	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.
326				"	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.

	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Ver 5.2 Location and/or New Requirement/Date	Topic	Shall Statement
327	New (2012) 5.5.7.4	5.5.7.4	5.5.7.4	Bluetooth (continued)	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.
328				"	12. Configure encryption key sizes to the maximum allowable. Using maximum allowable key sizes provides protection from brute force attacks.
329				"	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.
330				"	14. Use Security Mode 3 in order to provide link-level security prior to link establishment.
331				"	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 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Ver 5.2 Location and/or New Requirement/Date	Topic	Shall Statement
<b>CJIS Security Policy Area 6 - Identification and Authentication</b>					
332	New (2012) 5.6	5.6	5.6	Policy Area 6: Identification and Authentication	The agency <b>shall</b> 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.
333	5.6.1	5.6.1	5.6.1	Identification Policy and Procedures	Each person who is authorized to store, process, and/or transmit CJI <b>shall</b> be uniquely identified.
334	5.6.1			"	A unique identification <b>shall</b> also be required for all persons who administer and maintain the system(s) that access CJI or networks leveraged for CJI transit.
335	5.6.1			"	Agencies <b>shall</b> require users to identify themselves uniquely before the user is allowed to perform any actions on the system.
336	5.6.1			"	Agencies <b>shall</b> ensure that all user IDs belong to currently authorized users.
337	5.6.1			"	Identification data <b>shall</b> be kept current by adding new users and disabling and/or deleting former users.
338	5.6.1.1			5.6.1.1	5.6.1.1
339	5.6.1.1	"	The original identifier between the requesting agency and the CSA/SIB/Channeler <b>shall</b> be the ORI, and other agency identifiers, such as user identification or personal identifier, an access device mnemonic, or the Internet Protocol (IP) address.		
340	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 <b>shall</b> ensure that the ORI for each transaction can be traced, via audit trail, to the specific agency which is requesting the transaction.		
341	5.6.1.1	"	Agencies assigned a P (limited access) ORI <b>shall not</b> use the full access ORI of another agency to conduct an inquiry transaction.		
342	New (2011) 5.6.2	5.6.2	5.6.2		
343	5.6.2			"	The authentication strategy <b>shall</b> be part of the agency's audit for policy compliance.
344	5.6.2			"	The FBI CJIS Division <b>shall</b> identify and authenticate all individuals who establish direct web-based interactive sessions with FBI CJIS Services.
345	New (2011) 5.6.2			"	The FBI CJIS Division <b>shall</b> 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.
346			5.6.2.1	<i>Standard Authenticators</i>	<i>Agencies shall not allow the same authenticator to be used multiple times on a device or system.</i>
347	5.6.2.1	5.6.2.1	5.6.2.1.1	Password	Agencies <b>shall</b> follow the secure password attributes, below, to authenticate an individual's unique ID.
				"	Passwords <b>shall</b> :
348	5.6.2.1			"	1. Be a minimum length of eight (8) characters on all systems.
349				"	2. Not be a dictionary word or proper name.

	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Ver 5.2 Location and/or New Requirement/Date	Topic	Shall Statement
350	5.6.2.1	5.6.2.1	5.6.2.1.1	Password (continued)	3. Not be the same as the Userid.
351				"	4. Expire within a maximum of 90 calendar days.
352	5.6.2.1			"	5. Not be identical to the previous ten (10) passwords.
353				"	6. Not be transmitted in the clear outside the secure location.
354	New (2012) 5.6.2.1			"	7. Not be displayed when entered.
355	New (2012) 5.6.2.2.1	5.6.2.2.1	5.6.2.2.1	Advanced Authentication Policy and Rationale	AA <b>shall not</b> be required for users requesting access to CJI from within the perimeter of a physically secure location (Section 5.9), when the technical security controls have been met (Sections 5.5 and 5.10).
356				"	Conversely, if the technical security controls have not been met, AA <b>shall</b> be required even if the request for CJI originates from within a physically secure location.
357				"	<u>The two authentication factors shall be unique (i.e. password/token or biometric/password but not password/password or token/token).</u>
358	New (2012) 5.6.2.2.1	5.6.2.2.1		"	EXCEPTION: AA <b>shall</b> be required when the requested service has built AA into its processes and requires a user to provide AA before granting access.
359	5.6.3	5.6.3	5.6.3	Identifier and Authenticator Management	The agency <b>shall</b> establish identifier and authenticator management processes.
				Identifier Management	In order to manage user identifiers, agencies <b>shall</b> :
360	New (2012) 5.6.3.1	5.6.3.1	5.6.3.1	"	1. Uniquely identify each user.
361				"	2. Verify the identity of each user.
362				"	3. Receive authorization to issue a user identifier from an appropriate agency official.
363				"	4. Issue the user identifier to the intended party.
364				"	5. Disable the user identifier after a specified period of inactivity.
365				"	6. Archive user identifiers.
				Authenticator Management	In order to manage information system authenticators, agencies <b>shall</b> :
366	New (2012) 5.6.3.2	5.6.3.2	5.6.3.2	"	1. Define initial authenticator content.
367				"	2. Establish administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators.
368				"	3. Change default authenticators upon information system installation.
369				"	4. Change/refresh authenticators periodically.
370				"	Users <b>shall</b> 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.
				Assertions	Assertion mechanisms used to communicate the results of a remote authentication to other parties <b>shall</b> be:
371	New (2014) 5.6.4	5.6.4	5.6.4	"	1. Digitally signed by a trusted entity (e.g., the identity provider).
372				"	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.

	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Ver 5.2 Location and/or New Requirement/Date	Topic	Shall Statement
373	New (2014) 5.6.4	5.6.4	5.6.4	Assertions (continued)	Assertions generated by a verifier <b>shall</b> expire after 12 hours and...
374				"	...and <b>shall not</b> be accepted thereafter by the relying party.

	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Ver 5.2 Location and/or New Requirement/Date	Topic	Shall Statement
<b>CJIS Security Policy Area 7 - Configuration Management</b>					
375	New (2011) 5.7.1.1	5.7.1.1		Least Functionality	The agency <b>shall</b> configure the application, service, or information system to provide only essential capabilities and...
376	New (2011) 5.7.1.1			Least Functionality	...and <b>shall</b> specifically prohibit and/or restrict the use of specified functions, ports, protocols, and/or services.
377	5.7.1.2	5.7.1.2	5.7.1.2	Network Diagram	The agency <b>shall</b> 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.
				"	The network topological drawing <b>shall</b> include the following:
378	5.7.1.2			"	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.
379				"	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.
380				"	3. "For Official Use Only" (FOUO) markings.
381				New (2012) 5.7.1.2	"
382	New (2012) 5.7.2	5.7.2	5.7.2	Security of Configuration Documentation	Agencies <b>shall</b> protect the system documentation from unauthorized access consistent with the provisions described in section 5.5 Access Control.

	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Ver 5.2 Location and/or New Requirement/Date	Topic	Shall Statement
<b>CJIS Security Policy Area 8 - Media Protection</b>					
383	New (2011) 5.8	5.8	5.8	Policy Area 8: Media Protection	Media protection policy and procedures <b>shall</b> be documented and implemented to ensure that access to electronic and physical media in all forms is restricted to authorized individuals.
384	New (2011) 5.8			"	Procedures <b>shall</b> be defined for securely handling, transporting and storing media.
385	New (2011) 5.8.1	5.8.1	5.8.1	Media Storage and Access	The agency <b>shall</b> securely store electronic and physical media within physically secure locations or controlled areas.
386	New (2011) 5.8.1			"	The agency <b>shall</b> restrict access to electronic and physical media to authorized individuals.
387	New (2013) 5.8.1			"	If physical and personnel restrictions are not feasible then the data <b>shall</b> be encrypted per section 5.10.1.2.
388	New (2011) 5.8.2	5.8.2	5.8.2	Media Transport	The agency <b>shall</b> 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.
389	New (2011) 5.8.2.1	5.8.2.1	5.8.2.1	Electronic Media in Transit	Controls <b>shall</b> 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.
390	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 <b>shall</b> institute other controls to ensure the security of the data.
391	New (2011) 5.8.2.2	5.8.2.2	5.8.2.2	Physical Media in Transit	Physical media <b>shall</b> be protected at the same level as the information would be protected in electronic form.
392	5.8.3	5.8.3	5.8.3	Electronic Media Sanitization and Disposal	The agency <b>shall</b> sanitize, that is, overwrite at least three times or degauss electronic media prior to disposal or release for reuse by unauthorized individuals.
393	5.8.3			"	Inoperable electronic media <b>shall</b> be destroyed (cut up, shredded, etc.).
394	5.8.3			"	The agency <b>shall</b> maintain written documentation of the steps taken to sanitize or destroy electronic media.
395	New (2011) 5.8.3			"	Agencies <b>shall</b> ensure the sanitization or destruction is witnessed or carried out by authorized personnel.
396	New (2011) 5.8.4	5.8.4	5.8.4	Disposal of Physical Media	Physical media <b>shall</b> be securely disposed of when no longer required, using formal procedures.
397	New (2011) 5.8.4			"	Formal procedures for the secure disposal or destruction of physical media <b>shall</b> minimize the risk of sensitive information compromise by unauthorized individuals.
398	5.8.4			"	Physical media <b>shall</b> be destroyed by shredding or incineration.
399	New (2011) 5.8.4			"	Agencies <b>shall</b> ensure the disposal or destruction is witnessed or carried out by authorized personnel.

	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Ver 5.2 Location and/or New Requirement/Date	Topic	Shall Statement
<b>CJIS Security Policy Area 9 - Physical Protection</b>					
400	New (2011) 5.9	5.9	5.9	Policy Area 9: Physical Protection	Physical protection policy and procedures <b>shall</b> be documented and implemented to ensure CJI and information system hardware, software, and media are physically protected through access control measures.
401	New (2011) 5.9.1	5.9.1	5.9.1	Physically Secure Location	<b>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 30<sup>th</sup> 2014.</b>
402	5.9.1.1	5.9.1.1	5.9.1.1	Security Perimeter	The perimeter of physically secure location <b>shall</b> be prominently posted and separated from non-secure locations by physical controls.
403				"	Security perimeters <b>shall</b> be defined, controlled and secured in a manner acceptable to the CSA or SIB.
404	New (2013) 5.9.1.2	5.9.1.2	5.9.1.2	Physical Access Authorizations	The agency <b>shall</b> 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...
405	New (2013) 5.9.1.2	5.9.1.2		"	...or <b>shall</b> issue credentials to authorized personnel.
406	5.9.1.3	5.9.1.3	5.9.1.3	Physical Access Control	The agency <b>shall</b> control all physical access points (except for those areas within the facility officially designated as publicly accessible) and...
407	New (2011) 5.9.1.3			"	...and <b>shall</b> verify individual access authorizations before granting access.
408	5.9.1.4	5.9.1.4	5.9.1.4	Access Control for Transmission Medium	The agency <b>shall</b> control physical access to information system distribution and transmission lines within the physically secure location.
409	5.9.1.5	5.9.1.5	5.9.1.5	Access Control for Display Medium	The agency <b>shall</b> control physical access to information system devices that display CJI and...
410	5.9.1.5			"	...and <b>shall</b> position information system devices in such a way as to prevent unauthorized individuals from accessing and viewing CJI.
411	5.9.1.6	5.9.1.6	5.9.1.6	Monitoring Physical Access	The agency <b>shall</b> monitor physical access to the information system to detect and respond to physical security incidents.
412	New (2011) 5.9.1.7	5.9.1.7	5.9.1.7	Visitor Control	The agency <b>shall</b> control physical access by authenticating visitors before authorizing escorted access to the physically secure location (except for those areas designated as publicly accessible).
413	New (2011) 5.9.1.7			"	The agency <b>shall</b> escort visitors at all times and monitor visitor activity.
414	New (2013) 5.9.1.9	5.9.1.9	<u>5.9.1.8</u>	Delivery and Removal	The agency <b>shall</b> authorize and control information system-related items entering and exiting the physically secure location.
415	New (2013) 5.9.2	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 <b>shall</b> designate an area, a room, or a storage container, as a "controlled area" for the purpose of day-to-day CJI access or storage.
				"	The agency <b>shall</b> , at a minimum:
416	New (2012) 5.9.2			"	1. Limit access to the controlled area during CJI processing times to only those personnel authorized by the agency to access or view CJI.
417				"	2. Lock the area, room, or storage container when unattended.
418				"	3. Position information system devices and documents containing CJI in such a way as to prevent unauthorized individuals from access and view.

	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Ver 5.2 Location and/or New Requirement/Date	Topic	Shall Statement
419	New (2012) 5.9.2	5.9.2	5.9.2	Controlled Area (continued)	4. Follow the encryption requirements found in section 5.10.1.1.2 for electronic storage (i.e. data "at rest") of CJI.

	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Ver 5.2 Location and/or New Requirement/Date	Topic	Shall Statement
<b>CJIS Security Policy Area 10 - Systems and Communications Protection and Information Integrity</b>					
420	5.10.1	5.10.1	5.10.1	Information Flow Enforcement	The network infrastructure <b>shall</b> control the flow of information between interconnected systems.
	New (2013) 5.10.1.1	5.10.1.1	5.10.1.1	Boundary Protection	The agency <b>shall</b> :
421	5.10.1.1			"	1. Control access to networks processing CJL.
422	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.
423	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.
424	New (2013) 5.10.1.1			"	4. Employ tools and techniques to monitor network events, detect attacks, and provide identification of unauthorized use.
425	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 <b>shall</b> "fail closed" vs. "fail open").
426	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 <b>shall</b> follow the guidance in section 5.10.3.2 to achieve separation.
427	5.10.1.2	5.10.1.2	5.10.1.2	Encryption	1. Encryption <b>shall</b> be a minimum of 128 bit.
428	5.10.1.2			"	2. When CJI is transmitted outside the boundary of the physically secure location, the data <b>shall</b> be immediately protected via cryptographic mechanisms (encryption).
429	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 <b>shall</b> be protected via cryptographic mechanisms (encryption).
430	5.10.1.2			"	4. When encryption is employed, the cryptographic module used <b>shall</b> be certified to meet FIPS 140-2 standards.
431	New (2013) 5.10.1.2			"	5. For agencies using public key infrastructure technology, the agency <b>shall</b> 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 <b>shall</b> :
432				"	a) Include authorization by a supervisor or a responsible official.
433		"	b) Be accomplished by a secure process that verifies the identity of the certificate holder.		
434		"	c) Ensure the certificate is issued to the intended party.		
435	New (2013) 5.10.1.3	5.10.1.3	5.10.1.3	Intrusion Detection Tools and Techniques	The agency <b>shall</b> implement network-based and/or host-based intrusion detection tools.
	New (2012) 5.10.1.3			"	The CSA/SIB <b>shall</b> , in addition:
436				"	1. Monitor inbound and outbound communications for unusual or unauthorized activities.

	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Ver 5.2 Location and/or New Requirement/Date	Topic	Shall Statement
437	New (2012) 5.10.1.3	5.10.1.3	5.10.1.3	Intrusion 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.
438				"	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	5.10.1.4	Voice over Internet Protocol	In addition to the security controls described in this document, the following additional controls <b>shall</b> be implemented when an agency deploys VoIP within a network that contains unencrypted CJI:
439				"	1. Establish usage restrictions and implementation guidance for VoIP technologies.
440				"	2. Document, monitor and control the use of VoIP within the agency.
441				"	3. Utilize Virtual Local Area Network (VLAN) technology to segment VoIP traffic from data traffic.
442			New 5.10.1.5	<i>Cloud Computing</i>	<i>The metadata derived from Criminal Justice Information <b>shall not</b> be used by and Cloud Provider for any purposes.</i>
443				"	<i>The Cloud Provider <b>shall be prohibited from</b> scanning any email or data files for the purpose of building analytics, data mining, advertising, or improving the services provided.</i>
444	New (2012) 5.10.3.1	5.10.3.1	5.10.3.1	Partitioning	The application, service, or information system <b>shall</b> separate user functionality (including user interface services) from information system management functionality.
445	New (2012) 5.10.3.1			"	The application, service, or information system <b>shall</b> 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	5.10.3.2	Virtualization	In addition to the security controls described in this policy, the following additional controls <b>shall</b> be implemented in a virtual environment:
446				"	1. Isolate the host from the virtual machine. In other words, virtual machine users cannot access host files, firmware, etc.
447				"	2. Maintain audit logs for all virtual machines and hosts and store the logs outside the hosts' virtual environment.
448				"	3. Virtual Machines that are Internet facing (web servers, portal servers, etc.) <b>shall</b> be physically separate from Virtual Machines that process CJI internally.
449				"	4. Device drivers that are "critical" <b>shall</b> be contained within a separate guest.
450	New (2011) 5.10.4.1	5.10.4.1	5.10.4.1	Patch Management	The agency <b>shall</b> identify applications, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws.
451	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) <b>shall</b> develop and implement a local policy that ensures prompt installation of newly released security relevant patches, service packs and hot fixes. <b>NOTE: Because firewalls were specifically called out in 4.5, audit will continue against firewalls.</b>

	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Ver 5.2 Location and/or New Requirement/Date	Topic	Shall Statement
452	New (2011) 5.10.4.1	5.10.4.1	5.10.4.1	Patch Management (continued)	The agency (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor) <b>shall</b> develop and implement a local policy that ensures prompt installation of newly released security relevant patches, service packs and hot fixes. <b>NOTE: This requirement calls out all network and computing devices including firewalls. Once informational auditing is completed, the firewall specific requirement will be removed.</b>
453	New (2012) 5.10.4.1			"	Patch requirements discovered during security assessments, continuous monitoring or incident response activities <b>shall</b> also be addressed expeditiously.
454	New (2012) 5.10.4.2	5.10.4.2	5.10.4.2	Malicious Code Protection	The agency <b>shall</b> implement malicious code protection that includes automatic updates for all systems with Internet access.
455	New (2012) 5.10.4.2			"	Agencies with systems not connected to the Internet <b>shall</b> implement local procedures to ensure malicious code protection is kept current (i.e. most recent update available).
456	5.10.4.2			"	The agency <b>shall</b> 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.
457	New (2011) 5.10.4.2			"	The agency <b>shall</b> ensure malicious code protection is enabled on all of the aforementioned critical points and information systems and resident scanning is employed.
458	New (2012) 5.10.4.3	5.10.4.3	5.10.4.3	Spam and Spyware Protection	The agency <b>shall</b> implement spam and spyware protection.
				"	The agency <b>shall</b> :
459	New (2012) 5.10.4.3			"	1. Employ spam protection mechanisms at critical information system entry points (e.g. firewalls, electronic mail servers, remote-access servers).
460				"	2. <b>Employ spyware protection at workstations, servers <u>and</u> mobile computing devices on the network.</b>
461		"	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.		
462	5.10.4.4	5.10.4.4	5.10.4.4	Personal Firewall	A personal firewall <b>shall</b> be employed on all devices that are mobile by design (i.e. laptops, handhelds, personal digital assistants, etc.).
				"	At a minimum, the personal firewall <b>shall</b> perform the following activities:
463	5.10.4.4			"	1. Manage program access to the Internet.
464				"	2. Block unsolicited requests to connect to the PC.
465				"	3. Filter Incoming traffic by IP address or protocol.
466				"	4. Filter Incoming traffic by destination ports.
467		"	5. Maintain an IP traffic log.		
468	New (2012) 5.10.4.5	5.10.4.5	5.10.4.5	Security Alerts and Advisories	The agency <b>shall</b> :
469				"	1. Receive information system security alerts/advisories on a regular basis. 2. Issue alerts/advisories to appropriate personnel.

	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Ver 5.2 Location and/or New Requirement/Date	Topic	Shall Statement
470	New (2012) 5.10.4.5	5.10.4.5	5.10.4.5	Security Alerts and Advisories (continued)	3. Document the types of actions to be taken in response to security alerts/advisories.
"				4. Take appropriate actions in response.	
"				5. Employ automated mechanisms to make security alert and advisory information available throughout the agency as appropriate.	
473	5.10.4.6	5.10.4.6	5.10.4.6	Information Input Restrictions	The agency <b>shall</b> restrict the information input to any connection to FBI CJIS services to authorized personnel only.

	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Ver 5.2 Location and/or New Requirement/Date	Topic	Shall Statement
<b>CJIS Security Policy Area 11 - Formal Audits</b>					
474	5.11.1.1	5.11.1.1	5.11.1.1	Triennial Compliance Audits by the FBI CJIS Division	The CJIS Audit Unit (CAU) <b>shall</b> conduct a triennial audit of each CSA in order to verify compliance with applicable statutes, regulations and policies.
475	5.11.1.1			"	This audit <b>shall</b> include a sample of CJAs and, in coordination with the SIB, the NCJAs.
476	New (2013) 5.11.1.1			"	The FBI CJIS Division <b>shall</b> also have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.
477	New (2013) 5.11.1.2	5.11.1.2	5.11.1.2	Triennial Security Audits by the FBI CJIS Division	This audit <b>shall</b> include a sample of CJAs and NCJAs.
				Audits by the CSA	Each CSA <b>shall</b> :
478	5.11.2	5.11.2	5.11.2	"	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.
479	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.
480				"	3. Have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.
481	5.11.3	5.11.3	5.11.3	Special Security Inquiries and Audits	All agencies having access to CJI <b>shall</b> permit an inspection team to conduct an appropriate inquiry and audit of any alleged security violations.
482	5.11.3			"	The inspection team <b>shall</b> be appointed by the APB and <b>shall</b> include at least one representative of the CJIS Division.
483	5.11.3			"	All results of the inquiry and audit <b>shall</b> be reported to the APB with appropriate recommendations.

	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Ver 5.2 Location and/or New Requirement/Date	Topic	Shall Statement	
<b>CJIS Security Policy Area 12 - Personnel Security</b>						
484	5.12.1.1	5.12.1.1	5.12.1.1	Minimum Screening Requirements for Individuals Requiring Access to CJJ	1. To verify identification, a state of residency and national fingerprint-based record checks <b>shall</b> be conducted within 30 days of assignment for all personnel who have direct access to CJJ and those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJJ.	
485		New (2013) 5.12.1.1		"	However, if the person resides in a different state than that of the assigned agency, the agency <b>shall</b> 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.	
486	New (2012) 5.12.1.1	5.12.1.1		"	When appropriate, the screening <b>shall</b> 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.	
487	5.12.1.1	5.12.1.1		"	2. All requests for access <b>shall</b> be made as specified by the CSO.	
488	5.12.1.1			"	All CSO designees <b>shall</b> be from an authorized criminal justice agency.	
489	5.12.1.1			"	3. If a felony conviction of any kind exists, the hiring authority in the Interface Agency <b>shall</b> deny access to CJJ.	
490	5.12.1.1			"	4. If a record of any other kind exists, access to CJJ <b>shall not</b> be granted until the CSO or his/her designee reviews the matter to determine if access is appropriate.	
491	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 <b>shall</b> review the matter to determine if access to CJJ is appropriate.	
492	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, <b>shall</b> review the matter to determine if CJJ access is appropriate.	
493	New (2011) 5.12.1.1			"	7. If the person already has access to CJJ and is subsequently arrested and or convicted, continued access to CJJ <b>shall</b> be determined by the CSO.	
494	5.12.1.1			"	8. If the CSO or his/her designee determines that access to CJJ by the person would not be in the public interest, access <b>shall</b> be denied and the person's appointing authority shall be notified in writing of the access denial.	
495	5.12.1.1			"	8. If the CSO or his/her designee determines that access to CJJ by the person would not be in the public interest, access shall be denied and the person's appointing authority <b>shall</b> be notified in writing of the access denial.	
496	5.12.1.1			"	9. Support personnel, contractors, and custodial workers with access to physically secure locations or controlled areas (during CJJ processing) <b>shall</b> be subject to a state and national fingerprint-based record check unless these individuals are escorted by authorized personnel at all times.	
	5.12.1.2	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 <b>shall</b> meet the following requirements:
497	5.12.1.2	5.12.1.2			"	1. Prior to granting access to CJJ, the CGA on whose behalf the Contractor is retained <b>shall</b> verify identification via a state of residency and national fingerprint based record checks.

	Ver 5.0 Location and/or New Requirement/Date	Ver 5.1 Location and/or New Requirement/Date	Ver 5.2 Location and/or New Requirement/Date	Topic	Shall Statement	
498		New (2013) 5.12.1.2	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 <b>shall</b> 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.	
499	5.12.1.2	5.12.1.2		"	2. If a record of any kind is found, the CGA <b>shall</b> be formally notified, and...	
500	5.12.1.2			"	...and system access <b>shall</b> be delayed pending review of the criminal history record information.	
501	5.12.1.2			"	The CGA <b>shall</b> in turn notify the Contractor-appointed Security Officer.	
502	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) <b>shall</b> review the matter.	
503	New (2012) 5.12.1.2			"	4. A Contractor employee found to have a criminal record consisting of felony conviction(s) <b>shall</b> be disqualified.	
504	New (2012) 5.12.1.2			"	5. Applicants <b>shall</b> also be disqualified on the basis of confirmations that arrest warrants are outstanding for such applicants.	
505	New (2012) 5.12.1.2			5.12.1.2	"	6. The CGA <b>shall</b> maintain a list of personnel who have been authorized access to CJI and...
506	New (2012) 5.12.1.2				"	6. ...and <b>shall</b> , upon request, provide a current copy of the access list to the CSO.
507	New (2012) 5.12.1.2	5.12.2		5.12.2	Personnel Termination	The agency, upon termination of individual employment, <b>shall</b> immediately terminate access to CJI.
508	New (2012) 5.12.3	5.12.3	5.12.3	Personnel Transfer	The agency <b>shall</b> 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.	
509	5.12.4	5.12.4	5.12.4	Personnel Sanctions	The agency <b>shall</b> employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.	