Item	Year	Section	Old Section	Topic	Policy Statement
1	2011	4.3	New	Personally Identifiable Information (PN)	PII **shall** be extracted from CJI for the purpose of official business only.
2	2012		New		Agencies **shall** develop policies, based on state and local privacy rules, to ensure appropriate controls are applied when handling PII extracted from CJI.
		CJIS Security Policy Area 1 - Information Exchange Agreements			
	2008	5.1	Section 7.10(a) & 7.12(a) & 8.5	Information Exchange Agreements	The information shared through communication mediums **shall** be protected with appropriate security safeguards.
3	2011	5.1.1	New	Information Exchange	Before exchanging CJI, agencies **shall** put formal agreements in place that specify security controls.
4	2012		New		Information exchange agreements for agencies sharing CJI data that is sent to and/or received from the FBI CJIS **shall** specify the security controls and conditions described in this document.
5	2012		New		Information exchange agreements **shall** be supported by documentation committing both parties to the terms of information exchange.
6	2012	5.1.1.1	New	Information Handling	Procedures for handling and storage of information **shall** be established to protect that information from unauthorized disclosure, alteration or misuse.
7	2012		New		Using the requirements in this policy as a starting point, the procedures **shall** apply to the handling, processing, storing, and communication of CJI.
8	2012	5.1.2	New	Monitoring, Review, and Delivery of Services	As specified in the inter-agency agreements, MCAs, and contractual agreements with private contractors, the services, reports and records provided by the service provider **shall** be regularly monitored and reviewed.
9	2012		New		The **CJA shall** maintain sufficient overall control and visibility into all security aspects to include, but not limited to, identification of vulnerabilities and information security incident reporting/response.
10	2012		New		The incident reporting/response process used by the service provider **shall** conform to the incident reporting/response specifications provided in this policy.

11	2012	5.1.2.1	New	Managing Changes to Service Providers	Any changes to services provided by a service provider **shall** be managed by the CJA.
12	2012		New		Evaluation of the risks to the agency **shall** be undertaken based on the criticality of the data, system, and the impact of the change.
13	2012	5.1.3	New	Secondary Dissemination	If CHRI is released to another authorized agency, and that agency was not part of the releasing agency's primary information exchange agreement(s), the releasing agency **shall** log such dissemination.
		CJIS Security Policy Area 2 - Security Awareness Training			
14	2013	5.2	New	Security Awareness Training	Basic security awareness training **shall** be required within six months of initial assignment and biennially thereafter, for all personnel who have access to CJI.
15	2013	5.2.1.1	New	All Personnel	At a minimum, the following topics **shall** be addressed as baseline security awareness training for all authorized personnel with access to CJI:
16	2013	5.2.1.2	New	Personnel with Physical and Logical Access	In addition to 5.2.1.1 above, following topics at a minimum **shall** be addressed as baseline security awareness training for all authorized personnel with both physical and logical access to CJI:
17	2013	5.2.1.3	New	Personnel with Informatinon Technology Roles	In addition to 5.2.1.1 and 5.2.1.2 above, the following topics at a minimum **shall** be addressed as baseline security awareness training for all Information Technology personnel (system administrators, security administrators, network administrators, etc.):
		CJIS Security Policy Area 3 - Incident Response			
18	2012	5.3	New	Incident Response	Agencies **shall:** (i) establish an operational incident handling capability for agency information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; (ii) track, document, and report incidents to appropriate agency officials and/or authorities.
19	2012		New		ISOs have been identified as the POC on security-related issues for their respective agencies and **shall** ensure LASOs institute the CSA incident response reporting procedures at the local level.

20	2012	5.3.1	New	Reporting Information Security Events	The agency **shall** promptly report incident information to appropriate authorities.
21	2012		New		Information security events and weaknesses associated with information systems **shall** be communicated in a manner allowing timely corrective action to be taken.
22	2012		New		Wherever feasible, the agency **shall** employ automated mechanisms to assist in the reporting of security incidents.
23	2012		New		All employees, contractors and third party users **shall** be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of agency assets and are required to report any information security events and weaknesses as quickly as possible to the designated point of contact.
24	2012	5.3.2	New	Management of Information Security Incidents	A consistent and effective approach **shall** be applied to the management of information security incidents.
	2008		Section 5.3 & 5.4		Responsibilities and procedures **shall** be in place to handle information security events and weaknesses effectively once they have been reported.
25	2012	5.3.2.1	New	Incident Handling	The agency **shall** implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.
26	2013		New		Wherever feasible, the agency **shall** employ automated mechanisms to support the incident handling process.
27	2012	5.3.2.2	New	Collection of Evidence	Where a follow-up action against a person or agency after an information security incident involves legal action (either civil or criminal), evidence **shall** be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).
28	2012	5.3.3	New	Incident Response Training	The agency **shall** ensure general incident response roles responsibilities are included as part of required security awareness training.

29	2012	5.3.4	New	Incident Monitoring	The agency **shall** track and document information system security incidents on an ongoing basis.
		CJIS Security Policy Area 4 -Auditing and Accountability			
30	2013	5.4	New	Auditing and Accountability	Agencies **shall** implement audit and accountability controls to increase the probability of authorized users conforming to a prescribed pattern of behavior.
31	2013		New		Agencies **shall** carefully assess the inventory of components that compose their information systems to determine which security controls are applicable to the various components.
	2008	5.4.1	Section 7.14	Auditable Events and Content (Information Systems)	The agency's information system **shall** generate audit records for defined events.
32	2013		New		The agency **shall** specify which information system components carry out auditing activities.
	2008		Section 7.14		The agency's information system **shall** produce, at the application and/or operating system level, audit records containing sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.
33	2013		New		The agency **shall** periodically review and update the list of agency-defined auditable events.
34	2013		New		In the event an agency does not use an automated system, manual recording of activities **shall** still take place.
	2008	5.4.1.1	Section 7.14	Events	The following events **shall** be logged:
	2008		Section 7.14		1. Successful and unsuccessful system log-on attempts.
35	2013		New		2. Successful and unsuccessful attempts to access, create, write, delete or change permission on a user account, file, directory or other system resource.
36	2013		New		3. Successful and unsuccessful attempts to change account passwords.
37	2013		New		4. Successful and unsuccessful actions by privileged accounts.
38	2013		New		5. Successful and unsuccessful attempts for users to access, modify, or destroy the audit log file.
39	2013	5.4.1.1.1	New	Content	The following content **shall** be included with every audited event:
40	2013		New		1. Date and time of the event.
41	2013		New		2. The component of the information system (e.g., software component, hardware component) where the event occurred.

42	2013		New		3. Type of event.
43	2013		New		4. User/subject identity.
44	2013		New		5. Outcome (success or failure) of the event.
45	2013	5.4.2	New	Response to Audit Processing Failures	The agency's information system **shall** provide alerts to appropriate agency officials in the event of an audit processing failure.
46	2013	5.4.3	New	Audit Monitoring, Analysis, and Reporting	The responsible management official **shall** designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions.
47	2013		New		Audit review/analysis **shall** be conducted at a minimum once a week.
48	2013		New		The agency **shall** increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to agency operations, agency assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.
49	2013	5.4.4	New	Time Stamps	The agency's information system **shall** provide time stamps for use in audit record generation.
50	2013		New		The time stamps **shall** include the date and time values generated by the internal system clocks in the audit records.
51	2013		New		The agency **shall** synchronize internal information system clocks on an annual basis.
52	2013	5.4.5	New	Protection of Audit Information	The agency's information system **shall** protect audit information and audit tools from modification, deletion and unauthorized access.
53	2012	5.4.6	New	Audit Record Retention	The agency **shall** retain audit records for at least 365 days.
54	2013		New		Once the minimum retention time period has passed, the agency **shall** continue to retain audit records until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes.
		CJIS Security Policy Area 5 -Access Control			

55	2012	5.5.1	**New**	Account Management	The agency **shall** manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts.
56	2012		New		The agency **shall** validate information system accounts at least annually and **shall** document the validation process.
57	2013		**New**		The agency **shall** identify authorized users of the information system and specify access rights/privileges.
58	2013		New		The agency **shall** grant access to the information system based on:
59	2013		**New**		1. Valid need-to-know/need-to-share that is determined by assigned official duties.
60	2013		New		2. Satisfaction of all personnel security criteria.
61	2013		New		The agency responsible for account creation **shall** be notified when:
62	2013		**New**		1. A user's information system usage or need-to-know or need-to-share changes.
63	2013		**New**		2. A user is terminated or transferred or associated accounts are removed, disabled, or otherwise secured.
	2008	5.5.2	Section 7.6	Access Enforcement	The information system **shall** enforce assigned authorizations for controlling access to the system and contained information.
64	2012		**New**		The information system controls **shall** restrict access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel.
65	2013		**New**		Access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) **shall** be employed by agencies to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system.
66	2013	5.5.2.1	**New**	Least Privilege	The agency **shall** approve individual access privileges and **shall** enforce physical and logical access restrictions associated with changes to the information system; and generate, retain, and review records reflecting all such changes.

	2008		Section 7.6.3		The agency **shall** enforce the most restrictive set of rights/privileges or access needed by users for the performance of specified tasks.
	2008		Section 7.6.3		The agency **shall** implement least privilege based on specific duties, operations, or information systems as necessary to mitigate risk to CJI.
67	2013		New		Logs of access privilege changes **shall** be maintained for a minimum of one year or at least equal to the agency's record retention policy - whichever is greater.
68	2013	5.5.2.2	New	System Access Control	Access control mechanisms to enable access to CJI **shall** be restricted by object (e.g., data set, volumes, files, records) including the ability to read, write, or delete the objects.
69	2013		New		Access controls **shall** be in place and operational for all IT systems to:
70	2013		New		1. Prevent multiple concurrent active sessions for one user identification, for those applications accessing CJI, unless the agency grants authority based upon operational business needs. Agencies **shall** document the parameters of the operational business needs for multiple concurrent active sessions.
71	2013		New		2. Ensure that only authorized personnel can add, change, or remove component devices, dial-up connections, and remove or alter programs.
72	2013	5.5.2.3	New	Access Control Criteria	Agencies **shall** control access to CJI based on one or more of the following:
73	2013		New		1. Job assignment or function (i.e., the role) of the user seeking access.
74	2013		New		2. Physical location.
75	2013		New		3. Logical location.
76	2013		New		4. Network addresses (e.g., users from sites within a given agency may be permitted greater access than those from outside).
77	2013		New		5. Time-of-day and day-of-week/month restrictions.
78	2013	5.5.2.4	New	Access Control Mechanisms	When setting up access controls, agencies **shall** use one or more of the following mechanisms:

79	2013		New		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.
80	2013		New		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.
81	2013		New		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).
82	2013		New		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.
	2008	5.5.3	Section 7.6.1	Unsuccessful Login Attempts	Where technically feasible, the system **shall** enforce a limit of no more than 5 consecutive invalid access attempts by a user (attempting to access CJI or systems with access to CJI).
	2008		Section 7.6.1		The system **shall** automatically lock the account/node for a 10 minute time period unless released by an administrator.
83	2013	5.5.4	New	System Use Notification	The information system **shall** display an approved system use notification message, before granting access, informing potential users of various usages and monitoring rules.
84	2013		New		The system use notification message **shall,** at a minimum, provide the following information:
85	2013		New		1. The user is accessing a restricted information system.
86	2013		New		2. System usage may be monitored, recorded, and subject to audit.

87	2013		New		3. Unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties.
88	2013		New		4. Use of the system indicates consent to monitoring and recording.
89	2013		New		The system use notification message **shall** provide appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remain on the screen until the user acknowledges the notification and takes explicit actions to log on to the information system.
90	2013		New		Privacy and security policies **shall** be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.
	2008	5.5.5	Section 7.6.2	Session Lock	The information system **shall** prevent further access to the system by initiating a session lock after a maximum of 30 minutes of inactivity, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures.
91	2013		New		Users **shall** directly initiate session lock mechanisms to prevent inadvertent viewing when a device is unattended.
92	2013	5.5.6	New	Remote Access	The agency **shall** authorize, monitor, and control all methods of remote access to the information system.
93	2013		New		The agency **shall** employ automated mechanisms to facilitate the monitoring and control of remote access methods.
94	2013		New		The agency **shall** control all remote accesses through managed access control points.
95	2013		New		The agency may permit remote access for privileged functions only for compelling operational needs but **shall** document the rationale for such access in the security plan for the information system.
96	2011	5.5.6.1	New	Personally Owned Information Systems	A personally owned information system **shall not** be authorized to access, process, store or transmit CJI unless the agency has established and documented the specific terms and conditions for personally owned information system usage.
97	2012	5.5.7	New	Wireless Access Restrictions	The agency **shall:** (i) establish usage restrictions and implementation guidance for wireless technologies; and (ii) authorize, monitor, control wireless access to the information system.

98	2012	5.5.7.1	New	All 802.11x Wireless Protocols	Agencies **shall:**
99	2012		New		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.
100	2012		New		2. Maintain a complete inventory of all Access Points (APs) and 802.11 wireless devices.
101	2012		New		3. Place APs in secured areas to prevent unauthorized physical access and user manipulation.
102	2012		New		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.
103	2012		New		5. Enable user authentication and encryption mechanisms for the management interface of the AP.
104	2012		New		6. Ensure that all APs have strong administrative passwords and ensure that all passwords are changed in accordance with section 5.6.3.1.
105	2012		New		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.
106	2012		New		8. Change the default service set identifier (SS1D) in the APs. Disable the broadcast SSID feature so that the client SSID must match that of the AP. Validate that the SSID character string does not contain any agency identifiable information (division, department, street, etc.) or services.
107	2012		New		9. Enable all security features of the wireless product, including the cryptographic authentication, firewall, and other privacy features.
108	2012		New		10. Ensure that encryption key sizes are at least 128-bits and the default shared keys are replaced by unique keys.

109	2012		New		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.
110	2012		New		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.
111	2012		New		13. Enable logging (if supported) and review the logs on a recurring basis per local policy. At a minimum logs **shall** be reviewed monthly.
112	2012		New		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.
113	2012		New		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.
114	2012	5.5.7.2	New	Legacy 802.11 Protocols	Agencies **shall** follow the guidelines below regarding wireless implementation and cases where the WEP and WPA security features are used to provide wireless security in conjunction with the CJIS required minimum encryption specifications.
115	2012		New		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.
116	2012		New		2. Enable WEP/WPA.
117	2012		New		3. Ensure the default shared keys are replaced by more secure unique keys.
118	2012		New		4. Enable utilization of key-mapping keys rather than default keys so that sessions are unique when using WEP.
119	2012	5.5.7.3.1	New	Cellular Risk Mitigations	Organizations **shall,** as a minimum, ensure that cellular devices:
120	2012		New		1. Apply available critical patches and upgrades to the operating system.
121	2012		New		2. Are configured for local device authentication.
122	2012		New		3. Use advanced authentication.

123	2012		New		4. Encrypt all CJI resident on the device.
124	2012		New		5. Erase cached information when session is terminated.
125	2012		New		6. Employ personal firewalls.
126	2012		New		7. Employ antivirus software.
127	2012	5.5.7.4	New	Bluetooth	If such services are needed, they **shall** be provided through additional, higher-layer means in addition to the Bluetooth specification and 802.11 standards.
128	2012		New		Agencies **shall:**
129	2012		New		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.
130	2012		New		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.
131	2012		New		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.
132	2012		New		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).

133	2012	New	5. Choose personal identification number (PIN) codes that are sufficiently random and long. Avoid static and weak PfNs, such as all zeroes. PIN codes should be random so that they cannot be easily reproduced by malicious users. Longer PIN codes are more resistant to brute force attacks. For Bluetooth v2.0 (or earlier) devices, an eight-character alphanumeric PIN **shall** be used.
134	2012	New	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.
135	2012	New	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.
136	2012	New	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.
137	2012	New	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.
138	2012	New	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.

139	2012		New		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.
140	2012		New		12. Configure encryption key sizes to the maximum allowable. Using maximum allowable key sizes provides protection from brute force attacks.
141	2012		New		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.
142	2012		New		14. Use Security Mode 3 in order to provide link-level security prior to link establishment.
143	2012		New		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.
		CJfS Security Policy Area 6 - Identification and Authentication			
144	2012	5.6	New	Identification and Authentication	The agency **shall** identify information system users and processes acting on behalf of users and authenticate the identities of those users or processes as a prerequisite to allowing access to agency information systems or services.
145	2011	5.6.2	New	Authentication Policy and Procedures	Each individual's identity **shall** be authenticated at either the local agency, CSA, SIB or Channeler level.
146	2012	5.6.3.1	New	Identifier Management	The agency **shall** document and manage user identifiers by:
147	2012		New		1. Uniquely identifying each user.
148	2012		New		2. Verifying the identity of each user.
149	2012		New		3. Receiving authorization to issue a user identifier from an appropriate agency official.
150	2012		New		4. Issuing the user identifier to the intended party.

151	2012		New		5. Disabling the user identifier after a specified period of inactivity.
152	2012		New		6. Archiving user identifiers.
153	2012	5.6.3.2	New	Authenticator Management	In order to manage information system authenticators, agencies **shall:**
154	2012		New		1. Define initial authenticator content.
155	2012		New		2. Establish administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators.
156	2012		New		3. Change default authenticators upon information system installation.
157	2012		New		4. Change/refresh authenticators periodically.
158	2012		New		Users **shall** take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and immediately reporting lost or compromised authenticators.
159	2014	5.6.4	New	Assertions	Assertion mechanisms used to communicate the results of a remote authentication to other parties **shall** be:
160	2014		New		1. Digitally signed by a trusted entity (e.g., the identity provider).
161	2014		New		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.
162	2014		New		Assertions generated by a verifier **shall** expire after 12 hours and **shall not** be accepted thereafter by the relying party.
		CJIS Security Policy Area 7 - Configuration Management			
163	2011	5.7.1.1	New	Least Functionality	The agency **shall** configure the application, service, or information system to provide only essential capabilities and **shall** specifically prohibit and/or restrict the use of specified functions, ports, protocols, and/or services.
	2008	5.7.1.2	Section 7.1	Network Diagram	The agency **shall** ensure that a complete topological drawing depicting the interconnectivity of the agency network, to criminal justice information, systems and services is maintained in a current status.
	2008		Section 7.1		The network topological drawing **shall** include the following:

	2008		Section 7.1		1. All communications paths, circuits, and other components used for the interconnection, beginning with the agency-owned system(s) and traversing through all interconnected systems to the agency end-point.
	2008		Section 7.1		2. The logical location of all components (e.g., firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations). Individual workstations (clients) do not have to be shown; the number of clients is sufficient.
	2008		Section 7.1		3. "For Official Use Only" (FOUO) markings.
164	2012		New		4. The agency name and date (day, month, and year) drawing was created or updated.
165	2012	5.7.2	New	Security of Configuration Documentation	Agencies **shall** protect the system documentation from unauthorized access consistent with the provisions described in section 5.5 Access Control.
		CJIS Security Policy Area 8 - Media Protection			
166	2011	5.8	New	Media Protection	Media protection policy and procedures **shall** be documented and implemented to ensure that access to electronic and physical media in all forms is restricted to authorized individuals.
167	2011		New		Procedures **shall** be defined for securely handling, transporting and storing media.
168	2011	5.8.1	New	Media Storage and Access	The agency **shall** securely store electronic and physical media within physically secure locations or controlled areas.
169	2011		New		The agency **shall** restrict access to electronic and physical media to authorized individuals.
170	2013		New		If physical and personnel restrictions are not feasible then the data **shall** be encrypted per section 5.10.1.2.
171	2011	5.8.2	New	Media Transport	The agency **shall** protect and control electronic and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel.
172	2011	5.8.2.1	New	Electronic Media in Transit	Controls **shall** be in place to protect electronic media containing CJI while in transport (physically moved from one location to another) to help prevent compromise of the data.

173	2011		New		Encryption, as defined in section 5.10.1.2 of this policy, is the optimal control during transport; however, if encryption of the data isn't possible then each agency **shall** institute other controls to ensure the security of the data.
174	2011	5.8.2.2	New	Physical Media in Transit	Physical media **shall** be protected at the same level as the information would be protected in electronic form.
	2008	5.8.3	Section 4.6 & 4.7	Electronic Media Sanitization and Disposal	The agency **shall** sanitize, that is, overwrite at least three times or degauss electronic media prior to disposal or release for reuse by unauthorized individuals.
175	2011		New		Inoperable electronic media **shall** be destroyed (cut up, shredded, etc.).
176	2011		New		The agency **shall** maintain written documentation of the steps taken to sanitize or destroy electronic media.
177	2011		New		Agencies **shall** ensure the sanitization or destruction is witnessed or carried out by authorized personnel.
178	2011	5.8.4	New	Disposal of Physical Media	Physical media **shall** be securely disposed of when no longer required, using formal procedures.
179	2011		New		Formal procedures for the secure disposal or destruction of physical media **shall** minimize the risk of sensitive information compromise by unauthorized individuals.
	2008		Section 4.6		Physical media **shall** be destroyed by shredding or incineration.
180	2011		New		Agencies **shall** ensure the disposal or destruction is witnessed or carried out by authorized personnel.
		CJIS Security Policy Area 9 - Physical Protection			
181	2011	5.9	New	Policy Area 9: Physical Protection	Physical protection policy and procedures **shall** be documented and implemented to ensure CJI and information system hardware, software, and media are physically protected through access control measures.
182	2011	5.9.1	New	Physically Secure Location	For interim compliance, and for the sole purpose of meeting the advanced authentication policy, a police vehicle **shall** be considered a physically secure location until September 30 2013.
	2008	5.9.1.1	Section 7.2.2	Security Perimeter	The perimeter of physically secure location **shall** be prominently posted and separated from non-secure locations by physical controls.
	2008		Section 7.2.2		Security perimeters **shall** be defined, controlled and secured in a manner acceptable to the CSA or SIB.

183	2013	5.9.1.2	New	Physical Access Authorizations	The agency **shall** develop and keep current a list of personnel with authorized access to the physically secure location (except for those areas within the permanent facility officially designated as publicly accessible) or **shall** issue credentials to authorized personnel.
184	2011	5.9.1.3	New	Physical Access Control	The agency **shall** control all physical access points (except for those areas within the facility officially designated as publicly accessible) and **shall** verify individual access authorizations before granting access.
185	2011	5.9.1.4	New	Access Control for Transmission Medium	The agency **shall** control physical access to information system distribution and transmission lines within the physically secure location.
186	2011	5.9.1.7	New	Visitor Control	The agency **shall** control physical access by authenticating visitors before authorizing escorted access to the physically secure location (except for those areas designated as publicly accessible).
187	2011		New		The agency **shall** escort visitors at all times and monitor visitor activity.
188	2012	5.9.1.8	New	Access Records	The agency **shall** maintain visitor access records to the physically secure location (except for those areas officially designated as publicly accessible) that includes:
189	2012		New		1. Name and agency of the visitor.
190	2012		New		2. Signature of the visitor.
191	2012		New		3. Form of identification.
192	2012		New		4. Date of access.
193	2012		New		5. Time of entry and departure.
194	2012		New		6. Purpose of visit.
195	2012		New		7. Name and agency of person visited.
196	2012		New		The visitor access records **shall** be maintained for a minimum of one year.
197	2012		New		Designated officials within the agency **shall** frequently review the visitor access records for accuracy and completeness.
198	2013	5.9.1.9	New	Delivery and Removal	The agency **shall** authorize and control information system-related items entering and exiting the physically secure location.

199	2013	5.9.2	New	Controlled Area	If an agency cannot meet all of the controls required for establishing a physically secure location, but has an operational need to access or store CJI, the agency **shall** designate an area, a room, or a storage container, as a "'controlled area" for the purpose of day-to-day CJI access or storage.
200	2012		New		The agency **shall,** at a minimum:
201	2012		New		1. Limit access to the controlled area during CJI processing times to only those personnel authorized by the agency to access or view CJI.
202	2012		New		2. Lock the area, room, or storage container when unattended.
203	2012		New		3. Position information system devices and documents containing CJI in such a way as to prevent unauthorized individuals from access and view.
204	2012		New		4. Follow the encryption requirements found in section 5.10.1.1.2 for electronic storage (i.e. data "at rest") of CJI.
		CJIS Security Policy Area 10 - Systems and Communications Protection and Information Integrity			
	2008	5.10.1	Section 7.5	Information Flow Enforcement	The network infrastructure **shall** control the flow of information between interconnected systems.
205	2013	5.10.1.1	New	Boundary Protection	The agency **shall:**
	2008		Section 7		1. Control access to networks processing CJI.
206	2013		New		2. Monitor and control communications at the external boundary of the information system and at key internal boundaries within the system.
	2008		Section 7.5 & 7.13		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.
207	2013		New		4. Employ tools and techniques to monitor network events, detect attacks, and provide identification of unauthorized use.
208	2011		New		5. Ensure the operational failure of the boundary protection mechanisms do not result in any unauthorized release of information outside of the information system boundary (i.e. the device **shall** "fail closed" vs. "fail open").

209	2012		New		6. Allocate publicly accessible information system components (e.g. public Web servers) to separate sub networks with separate, network interfaces. Publicly accessible information systems residing on a virtual host **shall** follow the guidance in section 5.10.3.2 to achieve separation.
	2008	5.10.1.2	Section 7.9 & 7.12	Encryption	1. Encryption **shall** be a minimum of 128 bit.
	2008		Section 7.9		2. When CJI is transmitted outside the boundary **of** the physically secure location, the data **shall** be immediately protected via cryptographic mechanisms (encryption).
210	2013		New		3. When CJI is at rest (i.e. stored electronically) outside the boundary of the physically secure location, the data **shall** be protected via cryptographic mechanisms (encryption).
	2008		Section 7.9 & 7.12		4. When encryption is employed, the cryptographic module used **shall** be certified to meet FIPS 140-2 standards.
211	2013		New		5. For agencies using public key infrastructure technology, the agency **shall** develop and implement a certificate policy and certification practice statement for the issuance of public key certificates used in the information system.
212	2013		New		Registration to receive a public key certificate **shall:**
213	2013		New		a) Include authorization by a supervisor or a responsible official.
214	2013		New		b) Be accomplished by a secure process that verifies the identity of the certificate holder.
215	2013		New		c) Ensure the certificate is issued to the intended party.
216	2013	5.10.1.3	New	Intrustion Detection Tools and Techniques	The agency **shall** implement network-based and/or host-based intrusion detection tools.
217	2011	5.10.1.4	New	Voice over Internet Protocol	Agencies using the VoIP protocol **shall:**
218	2011		New		1. Establish usage restrictions and implementation guidance for VoIP technologies.
219	2011		New		2. Document, monitor and control the use of VoIP within the agency.
220	2012	5.10.3.1	New	Partitioning	The application, service, or information system **shall** separate user functionality (including user interface services) from information system management functionality.

221	2012		New		The application, service, or information system **shall** physically or logically separate user interface services (e.g. public Web pages) from information storage and management services (e.g. database management).
222	2012	5.10.3.2	New	Virtualization	In addition to the security controls described **in** this policy, the following additional controls **shall** be implemented in a virtual environment:
223	2012		New		1. Isolate the host from the virtual machine. In other words, virtual machine users cannot access host files, firmware, etc.
224	2012		New		2. Maintain audit logs for all virtual machines and hosts and store the logs outside the hosts' virtual environment.
225	2012		New		3. Virtual Machines that are Internet facing (web servers, portal servers, etc.) **shall** be physically separate from Virtual Machines that process CJI internally.
226	2012		New		4. Device drivers that are "critical" **shall** be contained within a separate guest.
227	2011	5.10.4.1	New	Patch Management	The agency **shall** identify applications, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws.
228	2011		New		The agency (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor) **shall** develop and implement a local policy that ensures prompt installation of newly released security relevant patches, service packs and hot fixes.
229	2012		New		Patch requirements discovered during security assessments, continuous monitoring or incident response activities **shall** also be addressed expeditiously.
230	2012	5.10.4.2	New	Malicious Code Protection	The agency **shall** implement malicious code protection that includes automatic updates for all systems with Internet access.
231	2012		New		Agencies with systems not connected to the Internet **shall** implement local procedures to ensure malicious code protection is kept current (i.e. most recent update available).

232	2008		Section 7.15		The agency **shall** employ virus protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses) at critical points throughout the network and on all workstations, servers and mobile computing devices on the network.
233	2011		New		The agency **shall** ensure malicious code protection is enabled on all of the aforementioned critical points and information systems and resident scanning is employed.
234	2012	5.10.4.3	New	Spam and Spyware Protection	The agency **shall** implement spam and spyware protection.
235	2012		New		The agency **shall:**
236	2012		New		1. Employ spam protection mechanisms at critical information system entry points (e.g. firewalls, electronic mail servers, remote-access servers).
237	2012		New		2. Employ spyware protection at workstations, servers or mobile computing devices on the network.
238	2012		New		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.
239	2012	5.10.4.5	New	Security Alerts and Advisories	The agency **shall:**
240	2012		New		1. Receive information system security alerts/advisories on a regular basis.
241	2012		New		2. Issue alerts/advisories to appropriate personnel.
242	2012		New		3. Document the types of actions to be taken in response to security alerts/advisories.
243	2012		New		4. Take appropriate actions in response.
244	2012		New		5. Employ automated mechanisms to make security alert and advisory information available throughout the agency as appropriate.
	2008	5.10.4.6	Section 7.6	Information Input Restrictions	The agency **shall** restrict the information input to any connection to FBI CJIS services to authorized personnel only.
		CJIS Security Policy Area 11 - Formal Audits			

	2008	5.11.1.1	Section 9.2	Triennial Compliance Audits by the FBI CJIS Division	The CJIS Audit Unit (CAU) **shall** conduct a triennial audit of each CSA in order to verify compliance with applicable statutes, regulations and policies.
	2008		Section 9.2		This audit **shall** include a sample of CJAs and, in coordination with the SIB, the NCJAs.
245	2013		New		The FBI CJIS Division shall also have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.
246	2013	5.11.1.2	New		This audit **shall** include a sample of CJAs and NCJAs.
	2008	5.11.2	Section 9.1	Audits by the CSA	Each CSA shall:
	2008		Section 9.1		1. At a minimum, triennially audit all CJAs and NCJAs which have direct access to the state system in order to ensure compliance with applicable statutes, regulations and policies.
247	2013		New		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.
248	2013		New		3. Have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.
		CJIS Security Policy Area 12 - Personnel Security			
249	2012	5.12.2	New	Personnel Termination	The agency, upon termination of individual employment, **shall** immediately terminate access to CJI.
250	2012	5.12.3	New	Personnel Transfer	The agency **shall** review CJI access authorizations when personnel are reassigned or transferred to other positions within the agency and initiate appropriate actions such as closing and establishing accounts and changing system access authorizations.
251	2012	5.12.4	New	Personnel Sanctions	The agency **shall** employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.