	Ver 5.5 Location and New Requirement	Ver 5.6 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
336	5.6.3.2	5.6.3.2	Authenticator Management (continued)	Users **shall** take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and immediately reporting lost or compromised authenticators.	1	Agency	Both	Both
	5.6.4	5.6.4	Assertions	Assertion mechanisms used to communicate the results of a remote authentication to other parties **shall** be:				
337			"	1. Digitally signed by a trusted entity (e.g., the identity provider).	1	Agency	Both	Both
338			"	2. Obtained directly from a trusted entity (e.g. trusted broker) using a protocol where the trusted entity authenticates to the relying party using a secure protocol (e.g. transport layer security [TLS]) that cryptographically authenticates the verifier and protects the assertion.	1	Agency	Both	Both
339			"	Assertions generated by a verifier **shall** expire after 12 hours and…	1	Agency	Both	Both
340			"	...and **shall not** be accepted thereafter by the relying party.	1	Agency	Both	Both

	Ver 5.5 Location and New Requirement	Ver 5.6 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy Area 7 - Configuration Management								
341	5.7.1.1	5.7.1.1	Least Functionality	The agency **shall** configure the application, service, or information system to provide only essential capabilities and…	2	Agency	Both	Both
342			"	...and **shall** specifically prohibit and/or restrict the use of specified functions, ports, protocols, and/or services.	1	Agency	Both	Both
343	5.7.1.2	5.7.1.2	Network Diagram	The agency **shall** ensure that a complete topological drawing depicting the interconnectivity of the agency network, to criminal justice information, systems and services is maintained in a current status.	1	Agency	Both	Both
			"	The network topological drawing **shall** include the following:				
344			"	1. All communications paths, circuits, and other components used for the interconnection, beginning with the agency-owned system(s) and traversing through all interconnected systems to the agency end-point.	1	Agency	Both	Both
345			"	2. The logical location of all components (e.g., firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations). Individual workstations (clients) do not have to be shown; the number of clients is sufficient.	1	Agency	Both	Both
346			"	3. “For Official Use Only” (FOUO) markings.	1	Agency	Both	Both
347			"	4. The agency name and date (day, month, and year) drawing was created or updated.	1	Agency	Both	Both
348	5.7.2	5.7.2	Security of Configuration Documentation	Agencies **shall** protect the system documentation from unauthorized access consistent with the provisions described in section 5.5 Access Control.	2	Agency	Both	Both

	Ver 5.5 Location and New Requirement	Ver 5.6 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy Area 8 - Media Protection								
349	5.8	5.8	Policy Area 8: Media Protection	Media protection policy and procedures **shall** be documented and implemented to ensure that access to electronic and physical media in all forms is restricted to authorized individuals.	2	Agency	Agency	Agency
350			"	Procedures **shall** be defined for securely handling, transporting and storing media.	2	Agency	Agency	Agency
351	5.8.1	5.8.1	Media Storage and Access	The agency **shall** securely store electronic and physical media within physically secure locations or controlled areas.	1	Both	Both	Both
352			"	The agency **shall** restrict access to electronic and physical media to authorized individuals.	1	Both	Both	Both
353			"	If physical and personnel restrictions are not feasible then the data **shall** be encrypted per section 5.10.1.2.	1	Both	Both	Both
354	5.8.2	5.8.2	Media Transport	The agency **shall** protect and control electronic and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel.	1	Agency	Agency	Agency
355	5.8.2.1	5.8.2.1	Electronic Media in Transit	Controls **shall** be in place to protect digital media containing CJI while in transport (physically moved from one location to another) to help prevent compromise of the data.	1	Agency	Agency	Agency
356			"	Encryption, as defined in section 5.10.1.2 of this policy, is the optimal control during transport; however, if encryption of the data isn't possible then each agency **shall** institute physical controls to ensure the security of the data.	1	Agency	Both	Both
357	5.8.2.2	5.8.2.2	Physical Media in Transit	Physical media **shall** be protected at the same level as the information would be protected in electronic form.	1	Agency	Agency	Agency
358	5.8.3	5.8.3	Electronic Media Sanitization and Disposal	The agency **shall** sanitize, that is, overwrite at least three times or degauss electronic media prior to disposal or release for reuse by unauthorized individuals.	1	Agency	Both	Both
359			"	Inoperable electronic media **shall** be destroyed (cut up, shredded, etc.).	1	Agency	Agency	Agency
360			"	The agency **shall** maintain written documentation of the steps taken to sanitize or destroy electronic media.	2	Agency	Agency	Agency
361			"	Agencies **shall** ensure the sanitization or destruction is witnessed or carried out by authorized personnel.	1	Agency	Agency	Agency
362	5.8.4	5.8.4	Disposal of Physical Media	Physical media **shall** be securely disposed of when no longer required, using formal procedures.	1	Agency	Agency	Agency
363			"	Formal procedures for the secure disposal or destruction of physical media **shall** minimize the risk of sensitive information compromise by unauthorized individuals.	2	Agency	Agency	Agency
364			"	Physical media **shall** be destroyed by shredding or incineration.	1	Agency	Agency	Agency
365			"	Agencies **shall** ensure the disposal or destruction is witnessed or carried out by authorized personnel.	1	Agency	Agency	Agency

	Ver 5.5 Location and New Requirement	Ver 5.6 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy Area 9 - Physical Protection								
366	5.9	5.9	Policy Area 9: Physical Protection	Physical protection policy and procedures **shall** be documented and implemented to ensure CJI and information system hardware, software, and media are physically protected through access control measures.	2	Both	Both	Both
367	5.9.1.1	5.9.1.1	Security Perimeter	The perimeter of physically secure location **shall** be prominently posted and separated from non-secure locations by physical controls.	1	Both	Both	Both
368			"	Security perimeters **shall** be defined, controlled and secured in a manner acceptable to the CSA or SIB.	1	Both	Both	Both
369	5.9.1.2	5.9.1.2	Physical Access Authorizations	The agency **shall** develop and keep current a list of personnel with authorized access to the physically secure location (except for those areas within the permanent facility officially designated as publicly accessible) or…	1	Both	Both	Both
370			"	...or **shall** issue credentials to authorized personnel.	1	Both	Both	Both
371	5.9.1.3	5.9.1.3	Physical Access Control	The agency **shall** control all physical access points (except for those areas within the facility officially designated as publicly accessible) and…	1	Both	Both	Both
372			"	...and **shall** verify individual access authorizations before granting access.	1	Both	Both	Both
373	5.9.1.4	5.9.1.4	Access Control for Transmission Medium	The agency **shall** control physical access to information system distribution and transmission lines within the physically secure location.	1	Both	Both	Both
374	5.9.1.5	5.9.1.5	Access Control for Display Medium	The agency **shall** control physical access to information system devices that display CJI and…	1	Both	Both	Both
375			"	...and **shall** position information system devices in such a way as to prevent unauthorized individuals from accessing and viewing CJI.	1	Both	Both	Both
376	5.9.1.6	5.9.1.6	Monitoring Physical Access	The agency **shall** monitor physical access to the information system to detect and respond to physical security incidents.	1	Both	Both	Both
377	5.9.1.7	5.9.1.7	Visitor Control	The agency **shall** control physical access by authenticating visitors before authorizing escorted access to the physically secure location (except for those areas designated as publicly accessible).	1	Both	Both	Both
378			"	The agency **shall** escort visitors at all times and monitor visitor activity.	1	Both	Both	Both
379	5.9.1.8	5.9.1.8	Delivery and Removal	The agency **shall** authorize and control information system-related items entering and exiting the physically secure location.	1	Both	Both	Both
380	5.9.2	5.9.2	Controlled Area	If an agency cannot meet all of the controls required for establishing a physically secure location, but has an operational need to access or store CJI, the agency **shall** designate an area, a room, or a storage container, as a “controlled area” for the purpose of day-to-day CJI access or storage.	1	Both	Both	Both
			"	The agency **shall**, at a minimum:				
381			"	1. Limit access to the controlled area during CJI processing times to only those personnel authorized by the agency to access or view CJI.	1	Both	Both	Both
382			"	2. Lock the area, room, or storage container when unattended.	1	Both	Both	Both
383			"	3. Position information system devices and documents containing CJI in such a way as to prevent unauthorized individuals from access and view.	1	Both	Both	Both
384			"	4. Follow the encryption requirements found in section 5.10.1.1.2 for electronic storage (i.e. data “at rest”) of CJI.	1	Both	Both	Both

	Ver 5.5 Location and New Requirement	Ver 5.6 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy Area 10 - Systems and Communications Protection and Information Integrity								
385	5.10.1	5.10.1	Information Flow Enforcement	The network infrastructure **shall** control the flow of information between interconnected systems.	1	Both	Service Provider	Service Provider
	5.10.1.1	5.10.1.1	Boundary Protection	The agency **shall**:				
386			"	1. Control access to networks processing CJI.	1	Both	Service Provider	Service Provider
387			"	2. Monitor and control communications at the external boundary of the information system and at key internal boundaries within the system.	1	Both	Service Provider	Service Provider
388			"	3. Ensure any connections to the Internet, other external networks, or information systems occur through controlled interfaces (e.g. proxies, gateways, routers, firewalls, encrypted tunnels). See Section 5.10.4.4 for guidance on personal firewalls.	1	Both	Service Provider	Service Provider
389			"	4. Employ tools and techniques to monitor network events, detect attacks, and provide identification of unauthorized use.	1	Both	Service Provider	Service Provider
390			"	5. Ensure the operational failure of the boundary protection mechanisms do not result in any unauthorized release of information outside of the information system boundary (i.e. the device **shall** "fail closed" vs. "fail open").	1	Both	Service Provider	Service Provider
391			"	6. Allocate publicly accessible information system components (e.g. public Web servers) to separate sub networks with separate, network interfaces. Publicly accessible information systems residing on a virtual host **shall** follow the guidance in section 5.10.3.2 to achieve separation.	1	Both	Service Provider	Service Provider
	5.10.1.2		~~Encryption~~	~~1. Encryption **shall** be a minimum of 128 bit.~~				
392		***5.10.1.2.1***	***Encryption for CJI in Transit***	~~2.~~ When CJI is transmitted outside the boundary of the physically secure location, the data **shall** be immediately protected via ~~cryptographic mechanisms (~~encryption~~)~~.	1	Both	Service Provider	Service Provider
393			"	***When encryption is employed, the cryptographic module used shall be FIPS 140-2 certified and …***	1	Both	Service Provider	Service Provider
394			"	***… and use a symmetric cipher key strength of at least 128 bit strength to protect CJI.***	1	Both	Service Provider	Service Provider
			"	b) Encryption **shall not** be required if the transmission medium meets all of the following requirements:				
395			"	i. The agency owns, operates, manages, or protects the medium.	1	Agency	Agency	Agency
396			"	ii. Medium terminates within physically secure locations at both ends with no interconnections between.	1	Agency	Agency	Agency
397			"	iii. Physical access to the medium is controlled by the agency using the requirements in Section 5.9.1 and 5.12.	1	Agency	Agency	Agency
398			"	iv. Protection includes safeguards (e.g. acoustic, electric, electromagnetic, and physical) and if feasible countermeasures (e.g. alarms, notifications) to permit its use for the tranmission of unencrypted information through an area of lesser classification or control.	1	Agency	Agency	Agency
399			"	v. With approval of the CSO.	1	Agency	Agency	Agency
400		***5.10.1.2.2***	***Encryption for CJI at Rest***	~~3.~~ When CJI is at rest (i.e. stored electronically) outside the boundary of the physically secure location, the data **shall** be protected via ~~cryptographic mechanisms (~~encryption~~)~~.	1	Both	Service Provider	Service Provider
401			"	***When encryption is employed, agencies shall either encrypt CJI in accordance with the standard in Section 5.10.1.2.1 above, or …***	1	Both	Service Provider	Service Provider
402			"	***… or use a symmetric cipher that is FIPS 197 certified (AES) and at least 256 bit strength.***	1	Both	Service Provider	Service Provider
			"	a) When agencies implement encryption on CJI at rest, the passphrase to unlock the cipher **shall** meet the following requirements:				

	Ver 5.5 Location and New Requirement	Ver 5.6 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
403	5.10.1.2	***5.10.1.2.2***	***Encryption for CJI at Rest (continued)***	i. Be at least 10 characters	1	Both	Service Provider	Service Provider
404			"	ii. Not be a dictionary word	1	Both	Service Provider	Service Provider
405			"	iii. Include at least one (1) upper case letter, one (1) lower case letter, one (1) number, and one (1) special character	1	Both	Service Provider	Service Provider
406			"	iv. Be changed when previously authorized personnel no longer require access	1	Both	Service	Service
407			"	b) Multiple files maintained in the same unencrypted folder **shall** have separate and distinct passphrases.	1	Both	Service Provider	Service Provider
408			"	b) All audit requirements found in Section 5.4.1 Auditable Events and Content (Information Systems) **shall** be applied.	1	Both	Service Provider	Service Provider
				~~4. When encryption is employed, the cryptographic module used **shall** be certified to meet FIPS 140-2 standards.~~				
409		***5.10.1.2.3***	***Public Key Infrastructure (PKI) Technology***	~~5.~~ For agencies using public key infrastructure ***(PKI)*** technology, the agency **shall** develop and implement a certificate policy and certification practice statement for the issuance of public key certificates used in the information	1	Both	Service Provider	Service Provider
			"	Registration to receive a public key certificate **shall**:				
410			"	a) Include authorization by a supervisor or a responsible official.	1	Both	Service Provider	Service Provider
411			"	b) Be accomplished by a secure process that verifies the identity of the certificate holder.	1	Both	Service Provider	Service Provider
412			"	c) Ensure the certificate is issued to the intended party.	1	Both	Service Provider	Service Provider
413	5.10.1.3	5.10.1.3	Intrustion Detection Tools and Techniques	The agency **shall** implement network-based and/or host-based intrusion detection tools.	1	Both	Service Provider	Service Provider
			"	The CSA/SIB **shall**, in addition:				
414			"	1. Monitor inbound and outbound communications for unusual or unauthorized activities.	1	Both	Service Provider	Service Provider
415			"	2. Send individual intrusion detection logs to a central logging facility where correlation and analysis will be accomplished as a system wide intrusion detection effort.	1	Both	Service Provider	Service Provider
416			"	3. Employ automated tools to support near-real-time analysis of events in support of detecting system-level attacks.	1	Both	Service Provider	Service Provider
	5.10.1.4	5.10.1.4	Voice over Internet Protocol	In addition to the security controls described in this document, the following additional controls **shall** be implemented when an agency deploys VoIP within a network that contains unencrypted CJI:				
417			"	1. Establish usage restrictions and implementation guidance for VoIP technologies.	1	Both	Service Provider	Service Provider
418			"	2. Document, monitor and control the use of VoIP within the agency.	1	Both	Service Provider	Service Provider
419			"	3. Utilize Virtual Local Area Network (VLAN) technology to segment VoIP traffic from data traffic.	1	Both	Service Provider	Service Provider
420	5.10.1.5	5.10.1.5	Cloud Computing	The metadata derived from Criminal Justice Information **shall not** be used by and Cloud Provider for any purposes.	1	Service Provider	Service Provider	Service Provider
421			"	The Cloud Provider **shall be prohibited from** scanning any email or data files for the purpose of building analytics, data mining, advertising, or improving the services provided.	1	Service Provider	Service Provider	Service Provider
422	***New 5.10.2***	5.10.2	Facsimile Transmission of CJI	CJI transmitted external to a physically secure location using a facsimile server, application or service which implements email-like technology, **shall** meet the encryption requirements for CJI in transit as defined in Section 5.10.	1	Both	Service Provider	Service Provider

	Ver 5.5 Location and New Requirement	Ver 5.6 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
423	5.10.3.1	5.10.3.1	Partitioning	The application, service, or information system **shall** separate user functionality (including user interface services) from information system management functionality.	2	Both	Service Provider	Service Provider
424			"	The application, service, or information system **shall** physically or logically separate user interface services (e.g. public Web pages) from information storage and management services (e.g. database management).	1	Both	Service Provider	Service Provider
	5.10.3.2	5.10.3.2	Virtualization	In addition to the security controls described in this policy, the following additional controls **shall** be implemented in a virtual environment:				
425			"	1. Isolate the host from the virtual machine. In other words, virtual machine users cannot access host files, firmware, etc.	1	Both	Service Provider	Service Provider
426			"	2. Maintain audit logs for all virtual machines and hosts and store the logs outside the hosts' virtual environment.	2	Both	Service Provider	Service Provider
427			"	3. Virtual Machines that are Internet facing (web servers, portal servers, etc.) **shall** be physically separate from Virtual Machines that process CJI internally *or be separated by a virtual firewall* .	1	Both	Service Provider	Service Provider
428			"	4. Drivers that serve critical functions **shall** be stored within the specific VM they service. In other words, do not store these drivers within the hypervisor, or host operating system, for sharing. Each VM is to be treated as an independent system - secured as independently as possible.	1	Both	Service Provider	Service Provider
	New 5.10.3.2		"	The following additional technical security controls **shall** be applied in virtual environments where CJI is comingled with non-CJI:				
429			"	1. Encrypt CJI when stored in a virtualized environment where CJI is comingled with non-CJI or segregate and store unencrypted CJI within its own secure VM.	1	Both	Service Provider	Service Provider
430			"	2. Encrypt network traffic within the virtual environment.	1	Both	Service Provider	Service Provider
431	5.10.4.1	5.10.4.1	Patch Management	The agency **shall** identify applications, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws.	1	Both	Service Provider	Service Provider
432			"	The agency (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor) **shall** develop and implement a local policy that ensures prompt installation of newly released security relevant patches, service packs and hot fixes.	1	Both	Service Provider	Service Provider
433			"	Patch requirements discovered during security assessments, continuous monitoring or incident response activities **shall** also be addressed expeditiously.	1	Both	Service Provider	Service Provider
434	5.10.4.2	5.10.4.2	Malicious Code Protection	The agency **shall** implement malicious code protection that includes automatic updates for all systems with Internet access.	1	Both	Service Provider	Service Provider
435			"	Agencies with systems not connected to the Internet **shall** implement local procedures to ensure malicious code protection is kept current (i.e. most recent update available).	1	Both	Service Provider	Service Provider
436	5.10.4.2	5.10.4.2	Malicious Code Protection (continued)	The agency **shall** employ virus protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses) at critical points throughout the network and on all workstations, servers and mobile computing devices on the network.	1	Both	Service Provider	Service Provider
437			"	The agency **shall** ensure malicious code protection is enabled on all of the aforementioned critical points and information systems and resident scanning is employed.	1	Both	Service Provider	Service Provider
438	5.10.4.3	5.10.4.3	Spam and Spyware Protection	The agency **shall** implement spam and spyware protection.	2	Both	Service Provider	Service Provider
			"	The agency **shall**:				
439			"	1. Employ spam protection mechanisms at critical information system entry points (e.g. firewalls, electronic mail servers, remote-access servers).	2	Both	Service Provider	Service Provider

	Ver 5.5 Location and New Requirement	Ver 5.6 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
440	5.10.4.3	5.10.4.3	Spam and Spyware Protection (continued)	2. Employ spyware protection at workstations, servers and mobile computing devices on the network.	2	Both	Service Provider	Service Provider
441			"	3. Use the spam and spyware protection mechanisms to detect and take appropriate action on unsolicited messages and spyware/adware, respectively, transported by electronic mail, electronic mail attachments, Internet accesses, removable media (e.g. diskettes or compact disks) or other removable media as defined in this policy document.	2	Both	Service Provider	Service Provider
	5.10.4.4	5.10.4.4	Security Alerts and Advisories	The agency **shall**:				
442			"	1. Receive information system security alerts/advisories on a regular basis.	2	Both	Service Provider	Service Provider
443			"	2. Issue alerts/advisories to appropriate personnel.	2	Both	Service Provider	Service Provider
444			"	3. Document the types of actions to be taken in response to security alerts/advisories.	2	Both	Service Provider	Service Provider
445			"	4. Take appropriate actions in response.	2	Both	Service Provider	Service Provider
446			"	5. Employ automated mechanisms to make security alert and advisory information available throughout the agency as appropriate.	2	Both	Service Provider	Service Provider
447	5.10.4.5	5.10.4.5	Information Input Restrictions	The agency **shall** restrict the information input to any connection to FBI CJIS services to authorized personnel only.	1	Agency	Agency	Agency

	Ver 5.5 Location and New Requirement	Ver 5.6 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy Area 11 - Formal Audits								
448	5.11.1.1	5.11.1.1	Triennial Compliance Audits by the FBI CJIS Division	The CJIS Audit Unit (CAU) **shall** conduct a triennial audit of each CSA in order to verify compliance with applicable statutes, regulations and policies.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
449			"	This audit **shall** include a sample of CJAs and, in coordination with the SIB, the NCJAs.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
450			"	The FBI CJIS Division **shall** also have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
451	5.11.1.2	5.11.1.2	Triennial Security Audits by the FBI CJIS Division	This audit **shall** include a sample of CJAs and NCJAs.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
	5.11.2	5.11.2	Audits by the CSA	Each CSA **shall**:				
452			"	1. At a minimum, triennially audit all CJAs and NCJAs which have direct access to the state system in order to ensure compliance with applicable statutes, regulations and policies.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
453			"	2. In coordination with the SIB, establish a process to periodically audit all NCJAs, with access to CJI, in order to ensure compliance with applicable statutes, regulations and policies.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
454			"	3. Have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
455	***New 5.11.2***		"	4. Have the authority, on behalf of another CSA, to conduct a CSP compliance audit of contractor facilities and provide the results to the requesting CSA. If a subsequent CSA requests an audit of the same contractor facility, the CSA may provide the results of the previous audit unless otherwise notified by the requesting CSA that a new audit be performed.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
456	5.11.3	5.11.3	Special Security Inquiries and Audits	All agencies having access to CJI **shall** permit an inspection team to conduct an appropriate inquiry and audit of any alleged security violations.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
457			"	The inspection team **shall** be appointed by the APB and **shall** include at least one representative of the CJIS Division.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO
458			"	All results of the inquiry and audit **shall** be reported to the APB with appropriate recommendations.	1	CJIS/CSO	CJIS/CSO	CJIS/CSO

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

	Ver 5.5 Location and New Requirement	Ver 5.6 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
477	5.12.1.2	5.12.1.2	Personnel Screening for Contractors and Vendors (continued)	The CGA **shall** in turn notify the Contractor-appointed Security Officer.	1	Agency	Agency	Agency
478			"	3. When identification of the applicant with a criminal history has been established by fingerprint comparison, the CGA or the CJA (if the CGA does not have the authority to view CHRI) **shall** review the matter.	1	Agency	Agency	Agency
479			"	4. A Contractor employee found to have a criminal record consisting of felony conv	1	Agency	Agency	Agency
480			"	5. Applicants **shall** also be disqualified on the basis of confirmations that arrest warrants are outstanding for such applicants.	1	Agency	Agency	Agency
481			"	6. The CGA **shall** maintain a list of personnel who have been authorized access to CJI and…	1	Agency	Agency	Agency
482			"	6. ...and **shall**, upon request, provide a current copy of the access list to the CSO.	1	Agency	Agency	Agency
483	5.12.2	5.12.2	Personnel Termination	The agency, upon termination of individual employment, **shall** immediately terminate access to CJI.	1	Both	Both	Both
484	5.12.3	5.12.3	Personnel Transfer	The agency **shall** review CJI access authorizations when personnel are reassigned or transferred to other positions within the agency and initiate appropriate actions such as closing and establishing accounts and changing system access authorizations.	1	Both	Both	Both
485	5.12.4	5.12.4	Personnel Sanctions	The agency **shall** employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.	2	Both	Both	Both

	Ver 5.5 Location and New Requirement	Ver 5.6 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy Area 13 - Mobile Devices								
			Mobile Devices	The agency **shall**:				
486	5.13	5.13	"	(i) establish usage restrictions and implementation guidance for mobile devices;	1	Agency	Agency	Agency
487			"	(ii) authorize, monitor, control wireless access to the information system.	1	Agency	Agency	Agency
488	5.13.1.1	5.13.1.1	802.11 Wireless Protocols	Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) cryptographic algorithms, used by all pre-80.11i protocols, do not meet the requirements for FIPS 140-2 and **shall not** be used.	1	Agency	Agency	Agency
489			"	Agencies **shall** implement the following controls for all agency-managed wireless access points with access to an agency's network that processes unencrypted CJI:	1	Agency	Agency	Agency
			"	Agencies **shall** implement the following controls for all agency-managed wireless access points:				
490			"	1. Perform validation testing to ensure rogue APs (Access Points) do not exist in the 802.11 Wireless Local Area Network (WLAN) and to fully understand the wireless network security posture.	1	Agency	Agency	Agency
491			"	2. Maintain a complete inventory of all Access Points (APs) and 802.11 wireless devices.	1	Agency	Agency	Agency
492			"	3. Place APs in secured areas to prevent unauthorized physical access and user manipulation.	1	Agency	Agency	Agency
493			"	4. Test AP range boundaries to determine the precise extent of the wireless coverage and design the AP wireless coverage to limit the coverage area to only what is needed for operational purposes.	1	Agency	Agency	Agency
494			"	5. Enable user authentication and encryption mechanisms for the management interface of the AP.	1	Agency	Agency	Agency
495			"	6. Ensure that all APs have strong administrative passwords and ensure that all passwords are changed in accordance with section 5.6.3.1.	1	Agency	Agency	Agency
496			"	7. Ensure the reset function on APs is used only when needed and is only invoked by authorized personnel. Restore the APs to the latest security settings, when the reset functions are used, to ensure the factory default settings are not utilized.	1	Agency	Agency	Agency
497			"	8. Change the default service set identifier (SSID) in the APs.	1	Agency	Agency	Agency
498			"	Disable the broadcast SSID feature so that the client SSID must match that of the AP.	1	Agency	Agency	Agency
499			"	Validate that the SSID character string does not contain any agency identifiable information (division, department, street, etc.) or services.	1	Agency	Agency	Agency
500			"	9. Enable all security features of the wireless product, including the cryptographic authentication, firewall, and other privacy features.	1	Agency	Agency	Agency
501			"	10. Ensure that encryption key sizes are at least 128-bits and…	1	Agency	Agency	Agency
502			"	...and the default shared keys are replaced by unique keys.	1	Agency	Agency	Agency
503			"	11. Ensure that the ad hoc mode has been disabled.	1	Agency	Agency	Agency
504			"	12. Disable all nonessential management protocols on the APs. Disable non-FIPS compliant secure access to the managment interface.	1	Agency	Agency	Agency
505			"	13. Ensure all management access and authentication occurs via FIPS compliant secure protocols (e.g. SFTP, HTTPS, SNMP over TLS, etc.). Disable non-FIPS compliant secure access to the managment interface.	1	Agency	Agency	Agency
506			"	14. Enable logging (if supported) and…	1	Agency	Agency	Agency
507			"	...and review the logs on a recurring basis per local policy.	1	Agency	Agency	Agency
508			"	At a minimum logs **shall** be reviewed monthly.	1	Agency	Agency	Agency

	Ver 5.5 Location and New Requirement	Ver 5.6 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
509	5.13.1.1	5.13.1.1	802.11 Wireless Protocols (continued)	15. Insulate, virtually (e.g. virtual local area network (VLAN) and ACLs) or physically (e.g. firewalls), the wireless network from the operational wired infrastructure.	1	Agency	Agency	Agency
510			"	16. When disposing of access points that will no longer be used by the agency, clear access point configuration to prevent disclosure of network configuration, keys, passwords, etc.	1	Agency	Agency	Agency
511	5.13.1.2.1	5.13.1.2.1	Cellular Service Abroad	When devices are authorized to access CJI outside the U.S., agencies **shall** perform an inspection to ensure that all controls are in place and functioning properly in accordance with the agency's policies prior to and after deployment outside of the U.S.	1	Agency	Agency	Agency
512	5.13.1.3	5.13.1.3	Bluetooth	Organizational security policy **shall** be used to dictate the use of Bluetooth and its associated devices based on the agency's operational and business processes.	2	Agency	Agency	Agency
	~~5.13.8~~ ***5.13.1.4***	5.13.1.4	Mobile Hotspots	When an agency allows mobile devices that are approved to access or store CJI to function as a Wi-Fi hotspot connecting to the Internet, they **shall** be configured:				
513			"	1. Enable encryption on the hotspot	1	Agency	Agency	Agency
514	***New 5.13.1.4***		"	2. Change the hotspot's default SSID	1	Agency	Agency	Agency
515			"	a. Ensure the hotspot SSID does not identify the device make/model or agency ownership	1	Agency	Agency	Agency
516			"	3. Create a wireless network password (Pre-shared key)	1	Agency	Agency	Agency
517			"	4. Enable the hotspot's port filtering/blocking features if present	1	Agency	Agency	Agency
518	~~5.13.8~~ ***5.13.1.4***		"	5. Only allow connections from agency controlled devices	1	Agency	Agency	Agency
519	***New 5.13.1.4***		"	OR 1. Have a MDM solution to provide the same security as identified in 1 - 5 above.	1	Agency	Agency	Agency
520	5.13.2	5.13.2	Mobile Device Management (MDM)	Devices that have had any unauthorized changes made to them (including but not limited to being rooted or jailbroken) **shall not** be used to process, store, or transmit CJI at any time.	1	Agency	Agency	Agency
			"	Agencies **shall** implement the following controls when allowing CJI access from devices running limited feature operating system:				
521			"	1. Ensure that CJI is only transferred between CJI authorized applications and storage areas of the device.	1	Agency	Agency	Agency
522			"	2. MDM with centralized administration configured and implemented to perform at least the:	1	Agency	Agency	Agency
523			"	i. Remote locking of the device	1	Agency	Agency	Agency
524			"	ii. Remote wiping of the device	1	Agency	Agency	Agency
525			"	iii. Setting and locking device configuration	1	Agency	Agency	Agency
526			"	iv. Detection of "rooted" and "jailbroken" devices	1	Agency	Agency	Agency
527			"	v. Enforcement of folder or disk level encryption	1	Agency	Agency	Agency
528			"	vi. Application of mandatory policy settings on the device	1	Agency	Agency	Agency
529			"	vii. Detection of unauthorized configurations	1	Agency	Agency	Agency
530			"	viii. Detection of unauthorized software or applications	1	Agency	Agency	Agency
531			"	ix. Ability to determine location of agency controlled devices	1	Agency	Agency	Agency
532			"	x. Prevention of unpatched devices from accessing CJI or CJI systems	1	Agency	Agency	Agency
533			"	xi. Automatic device wiping after a specified number of failed access attempts	1	Agency	Agency	Agency
	5.13.3	5.13.3	Wireless Device Risk Mitigations	Organizations **shall**, as a minimum, ensure that wireless devices:				
534			"	1. Apply available critical patches and upgrades to the operating system as soon as they become available for the device and after necessary testing as described in Section 5.10.4.1.	1	Agency	Agency	Agency

	Ver 5.5 Location and New Requirement	Ver 5.6 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
535	5.13.3	5.13.3	Wireless Device Risk Mitigations (continued)	2. Are configured for local device authentication (see Section 5.13.8.1).	1	Agency	Agency	Agency
536			"	3. Use advanced authentication or CSO approved compensating controls as per Section 5.13.7.2.1.	1	Agency	Agency	Agency
537			"	4. Encrypt all CJI resident on the device.	1	Agency	Agency	Agency
538			"	5. Erase cached information, to include authenticators (see Section 5.6.2.1) in applications, when session is terminated.	1	Agency	Agency	Agency
539			"	6. Employ personal firewalls or run a Mobile Device Management (MDM) system that facilitates the ability to provide firewall services from the agency level.	1	Agency	Agency	Agency
540			"	7. Employ malicious code protection or run a MDM system that facilitates the ability to provide anti-malware services from the agency level.	1	Agency	Agency	Agency
541	5.13.4.1	5.13.4.1	Patching/Updates	Agencies **shall** monitor mobile devices to ensure their patch and update state is current.	1	Agency	Agency	Agency
542	5.13.4.2	5.13.4.2	Malicious Code Protection	Agencies that allow smartphones and tablets to access CJI **shall** have a process to approve the use of specific software or applications on the devices.	1	Agency	Agency	Agency
543	~~5.13.4.4~~ ***5.13.4.3***	5.13.4.3	Personal Firewall	A personal firewall **shall** be employed on all devices that have a full-feature operating system (i.e. laptops or tablets with Windows or Linux/Unix operating systems).	1	Agency	Agency	Agency
			"	At a minimum, the personal firewall **shall** perform the following activities:				
544			"	1. Manage program access to the Internet.	1	Agency	Agency	Agency
545			"	2. Block unsolicited requests to connect to the PC.	1	Agency	Agency	Agency
546			"	3. Filter Incoming traffic by IP address or protocol.	1	Agency	Agency	Agency
547			"	4. Filter Incoming traffic by destination ports.	1	Agency	Agency	Agency
548			"	5. Maintain an IP traffic log.	1	Agency	Agency	Agency
549	5.13.5	5.13.5	Incident Response	In addition to the requirements in Section 5.3 Incident Response, agencies **shall** develop additional or enhanced incident reporting and handling procedures to address mobile device operating scenarios.	1	Agency	Agency	Agency
			"	Special reporting procedures for mobile devices **shall** apply in any of the following situations:				
550			"	1. Loss of device control. For example:	1	Agency	Agency	Agency
			"	a. Device known to be locked, minimal duration of loss				
			"	b. Device lock state unknown, minimal duration of loss				
			"	c. Device lock state unknown, extended duration of loss				
			"	d. Device known to be unlocked, more than momentary duration of loss				
551			"	2. Total loss of device	1	Agency	Agency	Agency
552			"	3. Device compromise	1	Agency	Agency	Agency
553			"	4. Device loss or compromise outside the United States	1	Agency	Agency	Agency
554	~~5.13.7~~ ***5.13.6***	5.13.6	Access Control	Access control (Section 5.5 Access Control) shall be accomplished by the application that accesses CJI.	1	Agency	Agency	Agency
555	~~5.13.9.1~~ ***5.13.7.1***	*5.13.7.1*	Local Device Authentication	When mobile devices are authorized for use in accessing CJI, local device authentication **shall** be used to unlock the device for use.	1	Agency	Agency	Agency
556			"	The authenticator used **shall** meet the requirements in section 5.6.2.1 Standard Authenticators.	1	Agency	Agency	Agency
557	***5.13.7.2***	5.13.7.2	Advance Authentication	When accessing CJI from an authorized mobile device, advanced authentication shall be used by the authorized user.	1	Agency	Agency	Agency
558	***5.13.7.2.1***	5.13.7.2.1	Compensating Controls	Before CSOs consider approval of compensating controls, Mobile Device Management (MDM) shall be implemented per Section 5.13.2.	1	Agency	Agency	Agency
			"	The compensating controls shall:				
559			"	1. Meet the intent of the CJIS Security Policy AA requirement	1	Agency	Agency	Agency

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