Sample Audit Checklist for CJIS Security Policy Area 2

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
5.2	**Security Awareness Training**					
1.	Based on inquiry and record examination, do all personnel[1] who have access to CJI/CHRI [2](which includes all personnel who have unescorted access to a physically secure location[3]) receive the required security awareness training (SAT) within six months of their initial assignment?	____	____	____	CSP 5.2.1	
2.	Based on inquiry and record examination, do all personnel who have access to CJI/CHRI (which includes all personnel who have unescorted access to a physically secure location) receive the required SAT, every two years after the initial training?	____	____	____	CSP 5.2.1	
3.	Based on record examination, were the following topics addressed as baseline SAT for all personnel who have unescorted access to a physically secure location?					
	1. Individual responsibilities and expected behavior with regard to being in the vicinity of CJI usage and/or terminals?	____	____	____	CSP 5.2.1.1(1)	
	2. Implications of noncompliance?	____	____	____	CSP 5.2.1.1(2)	
	3. Incident response (Identify points of contact and individual actions)?	____	____	____	CSP 5.2.1.1(3)	
	4. Visitor control and physical access to spaces—discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity, etc.?	____	____	____	CSP 5.2.1.1(4)	

[1] An individual, or group of individuals, who have been appropriately vetted through a national fingerprint-based record check and have been granted access to CJI/CHRI.

[2] The physical or logical (electronic) ability, right or privilege to view, modify or make use of CJI/CHRI.

[3] A facility, a criminal justice conveyance, or an area, a room, or a group of rooms, within a facility with both the physical and personnel security controls sufficient to protect CJI/CHRI and associated information systems.

Sample Audit Checklist for CJIS Security Policy Area 2

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
4.	Based on record examination, in addition to requirements identified in CSP 5.2.1.1, were the following topics addressed as baseline SAT for all authorized personnel with access to CJI/CHRI?					
	1. Media protection?	____	____	____	CSP 5.2.1.2(1)	
	2. Protect information subject to confidentiality concerns — hardcopy through destruction?	____	____	____	CSP 5.2.1.2(2)	
	3. Proper handling and marking of CJI?	____	____	____	CSP 5.2.1.2(3)	
	4. Threats, vulnerabilities, and risks associated with handling of CJI?	____	____	____	CSP 5.2.1.2(4)	
	5. Social engineering?	____	____	____	CSP 5.2.1.2(5)	
	6. Dissemination and destruction?	____	____	____	CSP 5.2.1.2(6)	
5.	Based on record examination, in addition to CSP 5.2.1.1 and CSP 5.2.1.2, were the following topics addressed as baseline SAT for all authorized personnel with both physical[4] and logical access[5] to CJI/CHRI?					
	1. Rules that describe responsibilities and expected behavior with regard to information system usage?	____	____	____	CSP 5.2.1.3(1)	
	2. Password usage and management—including creation, frequency of changes, and protection?	____	____	____	CSP 5.2.1.3(2)	
	3. Protection from viruses, worms, Trojan horses, and other malicious code?	____	____	____	CSP 5.2.1.3(3)	
	4. Unknown e-mail/attachments?	____	____	____	CSP 5.2.1.3(4)	
	5. Web usage—allowed versus prohibited; monitoring of user activity?	____	____	____	CSP 5.2.1.3(5)	
	6. Spam?	____	____	____	CSP 5.2.1.3(6)	
	7. Physical Security—increases in risks to systems and data?	____	____	____	CSP 5.2.1.3(7)	
	8. Handheld device security issues—address both physical and wireless security issues?	____	____	____	CSP 5.2.1.3(8)	
	9. Use of encryption and the transmission of sensitive/confidential information over the Internet—address agency policy, procedures, and technical contact for assistance?	____	____	____	CSP 5.2.1.3(9)	
	10. Laptop security—address both physical and information security issues?	____	____	____	CSP 5.2.1.3(10)	

[4] The physical ability, right or privilege to view, modify or make use of CJI/CHRI by means of physical presence within the proximity of computers and network devices (e.g. the ability to insert a boot disk or other device into the system, make a physical connection with electronic equipment, etc.).

[5] The technical means (e.g., read, create, modify, delete a file, execute a program, or use an external connection) for an individual or other computer system to utilize CJI/CHRI or CJIS applications.

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
	11. Personally owned equipment and software—state whether allowed or not (e.g., copyrights)?	____	____	____	CSP 5.2.1.3(11)	
	12. Access control issues—address least privilege and separation of duties?	____	____	____	CSP 5.2.1.3(12)	
	13. Individual accountability—explain what this means in the Tribe/TGRA?	____	____	____	CSP 5.2.1.3(13)	
	14. Use of acknowledgement statements—passwords, access to systems and data, personal use and gain?	____	____	____	CSP 5.2.1.3(14)	
	15. Desktop security—discuss use of screensavers, restricting visitors' view of information on screen (mitigating "shoulder surfing"), battery backup devices, allowed access to systems?	____	____	____	CSP 5.2.1.3(15)	
	16. Protect information subject to confidentiality concerns—in systems, archived, on backup media, and until destroyed?	____	____	____	CSP 5.2.1.3(16)	
	17. Threats, vulnerabilities, and risks associated with accessing CJIS Service systems and services?	____	____	____	CSP 5.2.1.3(17)	
6.	Based on record examination, in addition to CSP 5.2.1.1, CSP 5.2.1.2, and CSP 5.1.2.3, were the following topics addressed as baseline SAT for all Information Technology personnel (system administrators, security administrators, network administrators, etc.)?					
	1. Protection from viruses, worms, Trojan horses, and other malicious code—scanning, updating definitions?	____	____	____	CSP5 2.1.4(1)	
	2. Data backup and storage—centralized or decentralized approach?	____	____	____	CSP 5.2.1.4(2)	
	3. Timely application of system patches—part of configuration management?	____	____	____	CSP 5.2.1.4(3)	
	4. Access control measures?	____	____	____	CSP 5.2.1.4(4)	
	5. Network infrastructure protection measures?	____	____	____	CSP 5.2.1.4(5)	
7.	Based on inquiry and record examination, did the LASO(s) receive enhanced training as identified in CSP 5.2.2 prior to assuming the duties, but no later than six months after initial assignment?	____	____	____	CSP 5.2.2	
8.	Based on inquiry and record examination, does the LASO(s) receive enhanced training as identified in CSP 5.2.2, each year, after the initial training?	____	____	____	CSP 5.2.2	

Sample Audit Checklist for CJIS Security Policy Area 2

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
9.	Based on record examination, were the following topics addressed as enhanced SAT for a LASO:					
	1. The roles and responsibilities listed in CSP 3.2.9?	____	____	____	CSP 5.2.2(1)	
	2. Additional tribal/federal agency LASO roles and responsibilities?	____	____	____	CSP 5.2.2(2)	
	3. Summary of audit findings from previous NIGC CJIS audits?	____	____	____	CSP 5.2.2(3)	
	4. Findings from the last FBI CJIS Division audit?	____	____	____	CSP 5.2.2(4)	
	5. Most recent changes to the CSP.	____	____	____	CSP 5.2.2(5)	
10.	Based on records examination, are records of individual SAT and specific information system security training(s) documented, kept current and maintained?	____	____	____	CSP 5.2.3	