Sample Audit Checklist for the CJIS Security Policy (CJISSECPOL)

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
	Assessment, Authorization, Monitoring (CA)					
1.	Based on inquiry and record examination, has the Tribe or TGRA developed, documented, and disseminated to organizational personnel with assessment, authorization, and monitoring policy responsibilities:					
	• Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance?	____	____	____	CA-1, a.1. (a)	
	• Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines?	____	____	____	CA-1, a.1. (b)	
2.	Does the Tribe or TGRA have procedures to facilitate the implementation of the assessment, authorization, and monitoring policy and the associated assessment, authorization, and monitoring controls?	____	____	____	CA-1, a.2	
3.	Has the Tribe or TGRA designated organizational personnel with information security responsibilities to manage the development, documentation, and dissemination of the assessment, authorization, and monitoring policy and procedures?	____	____	____	CA-1, b	
4.	Based on inquiry and record examination, does the Tribe or TGRA review and update the current assessment, authorization, and monitoring:	____	____	____	CA-1, c.1	
	• Policy annually and following changes to the assessment criteria?					
	• Procedures annually and following changes to the assessment criteria?	____	____	____	CA-1, c.2	
5.	Based on inquiry and record examination, does the Tribe or TGRA select the appropriate assessor or assessment team for the type of assessment to be conducted?	____	____	____	CA-2, a	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
6.	Based on inquiry and record examination, has the Tribe or TGRA developed a control assessment plan that describes the scope of the assessment including:					
	1. Controls and control enhancements under assessment?	____	____	____	CA-2, b.1	
	2. Assessment procedures to be used to determine control effectiveness?	____	____	____	CA-2, b.2	
	3. Assessment environment, assessment team, and assessment roles and responsibilities?	____	____	____	CA-2, b.3	
7.	Based on inquiry and record examination, does the Tribe or TGRA ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment?	____	____	____	CA-2, c	
8.	Based on inquiry and record examination, has the Tribe or TGRA assessed the controls in the system and its environment of operation and any controls that have been impacted by evolving threats at least once every three years to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements?	____	____	____	CA-2, d	
9.	Based on inquiry and record examination, has the Tribe or TGRA produced a control assessment report that documents the results of the assessment?	____	____	____	CA-2, e	
10.	Based on inquiry and record examination, has the Tribe or TGRA provided the results of the control assessment report to the individual who executed the CJIS User Agreement (NIGC)?	____	____	____	CA-2, f	
11.	Based on inquiry and record examination, does the Tribe or TGRA employ independent assessors or assessment teams to conduct control assessments?	____	____	____	CA-2, (1)	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
12.	Based on inquiry and record examination, does the Tribe or TGRA, approve and manage the exchange of information between the agency system and external systems using the following agreements when applicable: 1. Agreements for Noncriminal Justice Use of CHRI: a. Security and Management Control Outsourcing Standard for Non-Channeling. Implementation is applicable to noncriminal justice administrative functions that do not require a direct connection to the FBI for submission of fingerprints and receipt of CHRI. Examples include making fitness determinations, processing, storing, or destroying documents, and maintaining IT platforms that do not connect to CJIS systems. Prior to implementation, did the Authorized Recipient (TGRA) receive written permission from the FBI Compact Officer? See the NIGC Sample Audit Checklist for Outsourcing.	____	____	____	CA-3, a.3	
13.	Based on inquiry and record examination, does the Tribe or TGRA document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated?	____	____	____	CA-3, b	
14.	Based on inquiry and record examination, does the Tribe or TGRA review and update the agreement(s) at least triennially or when responsibilities or signatories change?	____	____	____	CA-3, c	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
15.	Based on inquiry and record examination, does the Tribe or TGRA log the dissemination of CHRI (secondary dissemination), if applicable, in accordance with Section 17 of the 2021 CHRI MOU Guidance Appendix? Section 17 of the 2021 CHRI MOU Guidance Appendix reads: Dissemination Log - a. The TGRA shall document each release of a criminal history record, CJI, or CHRI in a dissemination log…, such as copies of a record released to an applicant, an applicant's attorney, or for purposes of an applicant's licensing or employment appeal hearing. This log shall include: i. Date of Dissemination ii. Applicant's Name iii. Provider's Name (Released By) iv. Requestor's Name & Released To v. SID/FBI Numbers vi. Reason for Dissemination (Why was this information requested? For what purpose?) vii. How the information was disseminated (email, fax, certified mail, etc.). See Final CHRI MOU.	____	____	____	CA-3, d 2021 CHRI MOU Guidance Appendix Section 17	
16.	Based on inquiry and record examination, has the Tribe or TGRA developed a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system?	____	____	____	CA-5, a	
17.	Based on inquiry and record examination, does the Tribe or TGRA update existing plan of action and milestones at least every six (6) months or when new information is available based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities?	____	____	____	CA-5, b	
18.	Based on inquiry and record examination, has the Tribe or TGRA assigned a senior official as the responsible official for the system?	____	____	____	CA-6, a	

Sample Audit Checklist for the CJIS Security Policy (CJISSECPOL)

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
19.	Based on inquiry and record examination, has the Tribe or TGRA assigned the senior official as the authorizing official for common controls available for inheritance by organizational systems?	____	____	____	CA-6, b	
20.	Based on inquiry and record examination, does the Tribe or TGRA ensure that the authorizing official for the system, before commencing operations:					
	1. Accepts the use of common controls inherited by the system?	____	____	____	CA-6, c.1	
	2. Authorizes the system to operate?	____	____	____	CA-6, c.2	
21.	Based on inquiry and record examination, does the Tribe or TGRA ensure that the authorizing official for common controls authorizes the use of those controls for inheritance by organizational systems?	____	____	____	CA-6, d	
22.	Based on inquiry and record examination, does the Tribe or TGRA update the authorizations at least every three (3) years?	____	____	____	CA-6, e	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
23.	Based on inquiry and record examination, has the Tribe or TGRA developed a system-level continuous monitoring strategy and implemented continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes:					
	1. AC-2(g) Account Management?	____	____	____	CA-7, a.1	
	2. AC-17(1) Remote Access | Monitoring and Control?	____	____	____	CA-7, a.2	
	3. AT-4(a) Training Records?	____	____	____	CA-7, a.3	
	4. CM-3(f) Configuration Change Control?	____	____	____	CA-7, a.4	
	5. CM-6(d) Configuration Settings?	____	____	____	CA-7, a.5	
	6. CM-11(c) User-Installed Software?	____	____	____	CA-7, a.6	
	7. IR-5 Incident Monitoring?	____	____	____	CA-7, a.7	
	8. MA-2(b) Controlled Maintenance?	____	____	____	CA-7, a.8	
	9. MA-3(a) Maintenance Tool?	____	____	____	CA-7, a.9	
	10. MA-4(a) Nonlocal Maintenance?	____	____	____	CA-7, a.10	
	11. PE-3(d) Physical Access Control?	____	____	____	CA-7, a.11	
	12. PE-6 Monitoring Physical Access?	____	____	____	CA-7, a.12	
	13. PE-14(b) Environmental Controls?	____	____	____	CA-7, a.13	
	14. PE-16 Delivery and Removal?	____	____	____	CA-7, a.14	
	15. PS-7(e) External Personnel Security?	____	____	____	CA-7, a.15	
	16. SA-9(c) External System Services?	____	____	____	CA-7, a.16	
	17. SC-7(a) Boundary Protection?	____	____	____	CA-7, a.17	
	18. SC-7(24)(b) Boundary Protection | Personally Identifiable Information?	____	____	____	CA-7, a.18	
	19. SC-18(b) Mobile Code?	____	____	____	CA-7, a.19	
	20. SI-4 System Monitoring?	____	____	____	CA-7, a.20	
	See related NIGC sample audit checklists at CJIS Resource Materials.					
24.	Based on inquiry and record examination, has the Tribe or TGRA established an ongoing frequency for monitoring and an ongoing frequency for assessment of control effectiveness?	____	____	____	CA-7, b	
25.	Based on inquiry and record examination, does the Tribe or TGRA conduct ongoing control assessments in accordance with the continuous monitoring strategy?	____	____	____	CA-7, c	
26.	Based on inquiry and record examination, does the Tribe or TGRA conduct ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy?	____	____	____	CA-7, d	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
27.	Based on inquiry and record examination, does the Tribe or TGRA correlate and conduct an analysis of information generated by control assessments and monitoring?	____	____	____	CA-7, e	
28.	Based on inquiry and record examination, does the Tribe or TGRA take response actions to address results of the analysis of control assessment and monitoring information?	____	____	____	CA-7, f	
29.	Based on inquiry and record examination, does the Tribe or TGRA report the security and privacy status of the system to organizational personnel with information security, privacy responsibilities, and system/network administrators annually, when security events/incidents occur, and when requested?	____	____	____	CA-7, g	
30.	Based on inquiry and record examination, does the Tribe or TGRA employ independent assessors or assessment teams to monitor the controls in the system on an ongoing basis?	____	____	____	CA-7, (1)	
31.	Based on inquiry and record examination, does the Tribe or TGRA ensure risk monitoring is an integral part of the continuous monitoring strategy that includes the following:					
	a. Effectiveness monitoring?	____	____	____	CA-7, (4)a	
	b. Compliance monitoring?	____	____	____	CA-7, (4)b	
	c. Change monitoring?	____	____	____	CA-7, (4)c	
32.	Based on inquiry and record examination, has the Tribe or TGRA authorized internal connections of components with the capability to process, store, or transmit CJI / CHRI to the system?	____	____	____	CA-9, a	
33.	Based on inquiry and record examination, does the Tribe or TGRA document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated?	____	____	____	CA-9, b	
34.	Based on inquiry and record examination, does the Tribe or TGRA terminate internal system connections when no longer required or authorized?	____	____	____	CA-9, c	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
35.	Based on inquiry and record examination, does the Tribe or TGRA review at least annually the continued need for each internal connection?	____	____	____	CA-9, d	