#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
	Configuration Management (CM)[1]					
1.	Based on inquiry and record examination, has the Tribe or TGRA developed, documented, and disseminated to organizational personnel with configuration management responsibilities an agency-level configuration management policy that:					
	• Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance?	____	____	____	CM-1, a.1.(a)	
	• Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines?	____	____	____	CM-1, a.1.(b)	
2.	Does the Tribe or TGRA have procedures[2] to facilitate the implementation of the configuration management policy and the associated configuration management controls?	____	____	____	CM-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 configuration management policy and procedures?	____	____	____	CM-1, b	
4.	Based on inquiry and record examination, has the Tribe or TGRA reviewed and updated the current configuration management:					
	• Policy annually and following any hardware or software changes to systems which process, store, or transmit Criminal Justice Information (CJI) / Criminal History Record Information (CHRI)?	____	____	____	CM-1, c.1	
	• Procedures annually and following any hardware or software changes to systems which process, store, or transmit CJI / CHRI?	____	____	____	CM-1, c.2	

[1] These requirements are auditable beginning October 1, 2024.

[2] *See* CJIS Security Policy, 5.7 *Configuration Management (CM)*, CM-1 *Policy and Procedures* ("Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. . . . Simply restating controls does not constitute an organizational policy or procedure.").

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
5.	Based on inquiry and record examination, does the Tribe or TGRA develop, document, and maintain under configuration control, a current baseline configuration of the system?	____	____	____	CM-2, a	
6.	Based on inquiry and record examination, does the Tribe or TGRA develop, document, and maintain a current and complete topological drawing depicting the interconnectivity of the agency network to CJI / CHRI systems and services?	____	____	____	CM-2, b	
7.	Based on inquiry and record examination, does the Tribe or TGRA review and update the baseline configuration and topological drawing of the system: • At least annually? • When required due to security-relevant changes to the system and/or security incidents occur? • When system components are installed or upgraded?	____ ____ ____	____ ____ ____	____ ____ ____	CM-2, c.1 CM-2, c.2 CM-2, c.3	
8.	Based on inquiry and record examination, does the Tribe or TGRA maintain the currency, completeness, accuracy, and availability of the baseline configuration of the system using automated mechanisms such as configuration management tools, hardware, software, firmware inventory tools, and network management tools?	____	____	____	CM-2, (2)	
9.	Based on inquiry and record examination, does the Tribe or TGRA retain at least one (1) previous version of baseline configurations of the system to support rollback?	____	____	____	CM-2, (3)	
10.	Based on inquiry and record examination, does the Tribe or TGRA issue devices (e.g., mobile devices) with CJISSECPOL compliant configurations to individuals traveling to locations that the organization deems to be of significant risk?	____	____	____	CM-2, (7) a	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
11.	Based on inquiry and record examination, does the Tribe or TGRA apply the following controls to the systems or components when the individuals return from travel: • Examine the device for signs of physical tampering, purge and reimage disk drives and/or devices as required and ensure all security controls are in place and functional?	____	____	____	CM-2, (7) b	
12.	Based on inquiry and record examination, does the Tribe or TGRA determine and document the types of changes to the system that are configuration-controlled?	____	____	____	CM-3, a	
13.	Based on inquiry and record examination, does the Tribe or TGRA review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses?	____	____	____	CM-3, b	
14.	Based on inquiry and record examination, does the Tribe or TGRA document configuration change decisions associated with the system?	____	____	____	CM-3, c	
15.	Based on inquiry and record examination, does the Tribe or TGRA implement approved configuration-controlled changes to the system?	____	____	____	CM-3, d	
16.	Based on inquiry and record examination, does the Tribe or TGRA retain records of configuration-controlled changes to the system for two (2) years?	____	____	____	CM-3, e	
17.	Based on inquiry and record examination, does the Tribe or TGRA monitor and review activities associated with configuration-controlled changes to the system?	____	____	____	CM-3, f	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
18.	Based on inquiry and record examination, does the Tribe or TGRA coordinate and provide oversight for configuration change control activities through personnel with configuration management responsibilities, a Configuration Control Board, or Change Advisory Board that convenes regularly or when hardware or software changes (i.e., updates, upgrades, replacements, etc.) to the information system are required?	____	____	____	CM-3, g	
19.	Based on inquiry and record examination, does the Tribe or TGRA test, validate, and document changes to the system before finalizing the implementation of the changes?	____	____	____	CM-3, (2)	
20.	Based on inquiry and record examination, does the Tribe or TGRA require organizational personnel with information security and privacy responsibilities to be members of the Configuration Control Board or Change Advisory Board?	____	____	____	CM-3, (4)	
21.	Based on inquiry and record examination, does the Tribe or TGRA analyze changes to the system to determine potential security and privacy impacts prior to change implementation?	____	____	____	CM-4	
22.	Based on inquiry and record examination, does the Tribe or TGRA, after-system changes, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security and privacy requirements for the system?	____	____	____	CM-4, (2)	
23.	Based on inquiry and record examination, does the Tribe or TGRA define, document, approve, and enforce physical and logical access restrictions associated with changes to the system?	____	____	____	CM-5	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
24.	Based on inquiry and record examination, does the Tribe or TGRA establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using established best practices and guidelines such as Defense Information Systems Agency (DISA) Secure Technical Implementation Guidelines (STIGs), Center for Internet Security (CIS) Benchmarks, or Federal Information Processing Standards?	____	____	____	CM-6, a	
25.	Based on inquiry and record examination, does the Tribe or TGRA implement the configuration settings?	____	____	____	CM-6, b	
26.	Based on inquiry and record examination, does the Tribe or TGRA identify, document, and approve any deviations from established configuration settings for system components that store, process, or transmit CJI / CHRI based on operational requirements?	____	____	____	CM-6, c	
27.	Based on inquiry and record examination, does the Tribe or TGRA monitor and control changes to the configuration settings in accordance with organizational policies and procedures?	____	____	____	CM-6, d	
28.	Based on inquiry and record examination, does the Tribe or TGRA configure the system to provide only essential capabilities to meet operational requirements?	____	____	____	CM-7, a	
29.	Based on inquiry and record examination, does the Tribe or TGRA prohibit or restrict the use of specified functions, ports, protocols, software, and/or services which are not required?	____	____	____	CM-7, b	
30.	Based on inquiry and record examination, does the Tribe or TGRA review the system annually, as the system changes, or incidents occur to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services?	____	____	____	CM-7, (1) a	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
31.	Based on inquiry and record examination, does the Tribe or TGRA disable or remove functions, ports, protocols, software, and/or services within the system deemed to be unnecessary and/or unsecure?	____	____	____	CM-7, (1) b	
32.	Based on inquiry and record examination, does the Tribe or TGRA prevent program execution in accordance with rules of behavior and/or rules authorizing the terms and conditions of software program usage?	____	____	____	CM-7, (2)	
33.	Based on inquiry and record examination, does the Tribe or TGRA identify software programs authorized to execute on the system?	____	____	____	CM-7, (5) a	
34.	Based on inquiry and record examination, does the Tribe or TGRA employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system?	____	____	____	CM-7, (5) b	
35.	Based on inquiry and record examination, does the Tribe or TGRA review and update the list of authorized software programs annually?	____	____	____	CM-7, (5) c	
36.	Based on inquiry and record examination, has the Tribe or TGRA developed and documented an inventory of system components that:					
	• Accurately reflects the system?	____	____		CM-8, a.1	
	• Includes all components within the system?	____	____		CM-8, a.2	
	• Does not include duplicate accounting of components or components assigned to any other system?	____	____		CM-8, a.3	
	• Is at the level of granularity deemed necessary for tracking and reporting?	____	____		CM-8, a.4	
	• Includes the following minimum information to achieve system component accountability: date of installation, model, serial number, manufacturer, supplier information, component type, software owner, software version number, software license information, and hardware and physical location?	____	____		CM-8, a.5	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
37.	Based on inquiry and record examination, does the Tribe or TGRA review and update the system component inventory annually?	____	____	____	CM-8, b	
38.	Based on inquiry and record examination, does the Tribe or TGRA update the inventory of system components as part of component installations, removals, and system updates?	____	____	____	CM-8, (1)	
39.	Based on inquiry and record examination, does the Tribe or TGRA detect the presence of unauthorized hardware, software, and firmware components within the system using automated mechanisms continuously or at least weekly?	____	____	____	CM-8, (3) a	
40.	Based on inquiry and record examination, does the Tribe or TGRA take the following actions when unauthorized components are detected: • Disable or isolate the unauthorized components and notify organizational personnel with security responsibilities?	____	____	____	CM-8, (3) b	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
41.	Based on inquiry and record examination, has the Tribe or TGRA developed, documented, and implemented a configuration management plan for the system that:					
	• Addresses roles, responsibilities, and configuration management processes and procedures?	____	____	____	CM-9, a	
	• Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items?	____	____	____	CM-9, b	
	• Defines the configuration items for the system and places the configuration items under configuration management?	____	____	____	CM-9, c	
	• Is reviewed and approved by organizational personnel with information security responsibilities and organizational personnel with configuration management responsibilities?	____	____	____	CM-9, d	
	• Protects the configuration management plan from unauthorized disclosure and modification?	____	____	____	CM-9, e	
42.	Based on inquiry and record examination, does the Tribe or TGRA use software and associated documentation in accordance with contract agreements and copyright laws?	____	____	____	CM-10, a	
43.	Based on inquiry and record examination, does the Tribe or TGRA track the use of software and associated documentation protected by quantity licenses to control copying and distribution?	____	____	____	CM-10, b	
44.	Based on inquiry and record examination, does the Tribe or TGRA control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work?	____	____	____	CM-10, c	
45.	Based on inquiry and record examination, does the Tribe or TGRA establish agency-level policies governing the installation of software by users?	____	____	____	CM-11, a	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
46.	Based on inquiry and record examination, does the Tribe or TGRA enforce software installation policies through automated methods?	____	____	____	CM-11, b	
47.	Based on inquiry and record examination, does the Tribe or TGRA monitor policy compliance through automated methods at least weekly?	____	____	____	CM-11, c	
48.	Based on inquiry and record examination, does the Tribe or TGRA identify and document the location of CJI / CHRI and the specific system components on which the information is processed, stored, or transmitted?	____	____	____	CM-12, a	
49.	Based on inquiry and record examination, does the Tribe or TGRA identify and document the users who have access to the system and system components where the information is processed and stored?	____	____	____	CM-12, b	
50.	Based on inquiry and record examination, does the Tribe or TGRA document changes to the location (i.e., system or system components) where the information is processed and stored?	____	____	____	CM-12, c	
51.	Based on inquiry and record examination, does the Tribe or TGRA use automated tools to identify CJI / CHRI on software and hardware system components to ensure controls are in place to protect organizational information and individual privacy?	____	____	____	CM-12, (1)	