#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
5.19	**Risk Assessment (RA)[1]**					
1.	Based on inquiry and record examination, has the Tribe or TGRA developed, documented, and disseminated to organizational personnel with risk assessment responsibilities an agency-level risk assessment policy that:					
	• Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance?	____	____	____	RA-1, a.1.(a)	
	• Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines?	____	____	____	RA-1, a.1.(b)	
2.	Does the Tribe or TGRA have procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls?	____	____	____	RA-1, a.2	
3.	Has the Tribe or TGRA designated organizational personnel with security and privacy responsibilities to manage the development, documentation, and dissemination of the risk assessment policy and procedures?	____	____	____	RA-1, b	
4.	Based on inquiry and record examination, does the Tribe or TGRA review and update the current risk assessment:					
	• Policy annually and following any security incidents involving unauthorized access to Criminal Justice Information (CJI) / Criminal History Record Information (CHRI) or systems used to process, store, or transmit CJI / CHRI, or training simulations or exercises?	____	____	____	RA-1, c.1	
	• Procedures annually and following any security incidents involving unauthorized access to CJI / CHRI or systems used to process, store, or transmit CJI / CHRI, or training simulations or exercises?	____	____	____	RA-1, c.2	

[1] These requirements are sanctionable for audit beginning October 1, 2024.

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
5.	Based on inquiry and record examination, has the Tribe or TGRA categorized[2] the system and information it processes, stores, and transmits?	____	____	____	RA-2, a	
6.	Based on inquiry and record examination, does the Tribe or TGRA document the security categorization results, including supporting rationale, in the security plan for the system?	____	____	____	RA-2, b	
7.	Based on inquiry and record examination, does the Tribe or TGRA verify that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision?	____	____	____	RA-2, c	

[2] Security categories describe the potential adverse impacts or negative consequences to organizational operations, organizational assets, and individuals if organizational information and systems are compromised through a loss of confidentiality, integrity, or availability. Security categorization is also a type of asset loss characterization in systems security engineering processes that is carried out throughout the system development life cycle. Organizations can use privacy risk assessments or privacy impact assessments to better understand the potential adverse effects on individuals. The FBI CJIS Advisory Policy Board (APB) has assigned a security categorization of "moderate" for CJI and systems that process, store, and transmit CJI.

Organizations conduct the security categorization process as an organization-wide activity with the direct involvement of chief information officers, senior agency information security officers, senior agency officials for privacy, system owners, mission and business owners, and information owners or stewards.

Security categorization processes facilitate the development of inventories of information assets and, along with CM-8, mappings to specific system components where information is processed, stored, or transmitted. The security categorization process is revisited throughout the system development life cycle to ensure that the security categories remain accurate and relevant.

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
8.	Based on inquiry and record examination, does the Tribe or TGRA conduct a risk assessment[3], including:					
	• Identifying threats to and vulnerabilities in the system?	____	____	____	RA-3, a.1	
	• Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information?	____	____	____	RA-3, a.2	
	• Determining the likelihood and impact of adverse effects on individuals arising from the processing of Personally Identifiable Information (PII)?	____	____	____	RA-3, a.3	
9.	Based on inquiry and record examination, does the Tribe or TGRA integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments?	____	____	____	RA-3, b	
10.	Based on inquiry and record examination, does the Tribe or TGRA document risk assessment results in a risk assessment report?	____	____	____	RA-3, c	
11.	Based on inquiry and record examination, does the Tribe or TGRA review risk assessment results at least quarterly?	____	____	____	RA-3, d	

[3] Risk assessments consider threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals, other organizations, and the Nation. Risk assessments also consider risk from external parties, including contractors who operate systems on behalf of the organization, individuals who access organizational systems, service providers, and outsourcing entities.

Organizations can conduct risk assessments at all three levels in the risk management hierarchy (i.e., organization level, mission/business process level, or information system level) and at any stage in the system development life cycle. Risk assessments can also be conducted at various steps in the Risk Management Framework, including preparation, categorization, control selection, control implementation, control assessment, authorization, and control monitoring. Risk assessment is an ongoing activity carried out throughout the system development life cycle.

Risk assessments can also address information related to the system, including system design, the intended use of the system, testing results, and supply chain-related information or artifacts. Risk assessments can play an important role in control selection processes, particularly during the application of tailoring guidance and in the earliest phases of capability determination.

#	QUESTION	YES	NO	N/A	STANDARD	COMMENT
12.	Based on inquiry and record examination, does the Tribe or TGRA disseminate risk assessment results to organizational personnel with risk assessment responsibilities and organizational personnel with security and privacy responsibilities?	____	____	____	RA-3, e	
13.	Based on inquiry and record examination, does the Tribe or TGRA update the risk assessment at least quarterly or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system?	____	____	____	RA-3, f	
14.	Based on inquiry and record examination, does the Tribe or TGRA monitor and scan for vulnerabilities in the system and hosted applications at least monthly and when new vulnerabilities potentially affecting the system are identified and reported?	____	____	____	RA-5, a	
15.	Based on inquiry and record examination, does the Tribe or TGRA employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:					
	• Enumerating platforms, software flaws, and improper configurations?	____	____	____	RA-5, b.1	
	• Formatting checklists and test procedures?	____	____	____	RA-5, b.2	
	• Measuring vulnerability impact?	____	____	____	RA-5, b.3	
16.	Based on inquiry and record examination, does the Tribe or TGRA analyze vulnerability scan reports and results from vulnerability monitoring[4]?	____	____	____	RA-5, c	

[4] Organizations determine the required vulnerability monitoring for system components, ensuring that the potential sources of vulnerabilities—such as infrastructure components (e.g., switches, routers, guards, sensors), networked printers, scanners, and copiers—are not overlooked. The capability to readily update vulnerability monitoring tools as new vulnerabilities are discovered and announced and as new scanning methods are developed helps to ensure that new vulnerabilities are not missed by employed vulnerability monitoring tools. The vulnerability monitoring tool update process helps to ensure that potential vulnerabilities in the system are identified and addressed as quickly as possible. Vulnerability monitoring and analyses for custom software may require additional approaches, such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Organizations can use these analysis approaches in source code reviews and in a variety of tools, including web-based application scanners, static analysis tools, and binary analyzers.

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
17.	Based on inquiry and record examination, does the Tribe or TGRA remediate legitimate vulnerabilities within the number of days listed:					
	• Critical–15 days?	____	____	____	RA-5, d	
	• High–30 days?	____	____	____	RA-5, d	
	• Medium–60 days?	____	____	____	RA-5, d	
	• Low–90 days?	____	____	____	RA-5, d	
18.	Based on inquiry and record examination, does the Tribe or TGRA share information obtained from the vulnerability monitoring process and control assessments with organizational personnel with risk assessment, control assessment, and vulnerability scanning responsibilities to help eliminate similar vulnerabilities in other systems?	____	____	____	RA-5, e	
19.	Based on inquiry and record examination, does the Tribe or TGRA employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned?	____	____	____	RA-5, f	

Vulnerability monitoring includes scanning for patch levels; scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and scanning for flow control mechanisms that are improperly configured or operating incorrectly. Vulnerability monitoring may also include continuous vulnerability monitoring tools that use instrumentation to continuously analyze components. Instrumentation-based tools may improve accuracy and may be run throughout an organization without scanning. Vulnerability monitoring tools that facilitate interoperability include tools that are Security Content Automated Protocol (SCAP)-validated. Thus, organizations consider using scanning tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that employ the Open Vulnerability Assessment Language (OVAL) to determine the presence of vulnerabilities. Sources for vulnerability information include the Common Weakness Enumeration (CWE) listing and the National Vulnerability Database (NVD). Control assessments, such as red team exercises, provide additional sources of potential vulnerabilities for which to scan. Organizations also consider using scanning tools that express vulnerability impact by the Common Vulnerability Scoring System (CVSS).

Vulnerability monitoring includes a channel and process for receiving reports of security vulnerabilities from the public at-large. Vulnerability disclosure programs can be as simple as publishing a monitored email address or web form that can receive reports, including notification authorizing good-faith research and disclosure of security vulnerabilities. Organizations generally expect that such research is happening with or without their authorization and can use public vulnerability disclosure channels to increase the likelihood that discovered vulnerabilities are reported directly to the organization for remediation.

Organizations may also employ the use of financial incentives (also known as "bug bounties") to further encourage external security researchers to report discovered vulnerabilities. Bug bounty programs can be tailored to the organization's needs. Bounties can be operated indefinitely or over a defined period of time and can be offered to the general public or to a curated group. Organizations may run public and private bounties simultaneously and could choose to offer partially credentialed access to certain participants in order to evaluate security vulnerabilities from privileged vantage points.

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
20.	Based on inquiry and record examination, does the Tribe or TGRA update the system vulnerabilities to be scanned within 24 hours prior to running a new scan or when new vulnerabilities are identified and reported?	____	____	____	RA-5, (2)	
21.	Based on inquiry and record examination, does the Tribe or TGRA implement privileged access authorization to information system components containing or processing CJI / CHRI for vulnerability scanning activities requiring privileged access?	____	____	____	RA-5, (5)	
22.	Based on inquiry and record examination, does the Tribe or TGRA establish a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components?	____	____	____	RA-5, (11)	
23.	Based on inquiry and record examination, does the Tribe or TGRA respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance?	____	____	____	RA-7	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
24.	Based on inquiry and record examination, does the Tribe or TGRA identify critical system components and functions by performing a criticality analysis[5] for information system components containing or processing CJI at the planning, design, development, testing, implementation, and maintenance stages of the system development life cycle?	____	____	____	RA-9	

[5] Not all system components, functions, or services necessarily require significant protections. For example, criticality analysis is a key tenet of supply chain risk management and informs the prioritization of protection activities. The identification of critical system components and functions considers applicable laws, executive orders, regulations, directives, policies, standards, system functionality requirements, system and component interfaces, and system and component dependencies. Systems engineers conduct a functional decomposition of a system to identify mission-critical functions and components. The functional decomposition includes the identification of organizational missions supported by the system, decomposition into the specific functions to perform those missions, and traceability to the hardware, software, and firmware components that implement those functions, including when the functions are shared by many components within and external to the system.

The operational environment of a system or a system component may impact the criticality, including the connections to and dependencies on cyber-physical systems, devices, system-of- systems, and outsourced IT services. System components that allow unmediated access to critical system components or functions are considered critical due to the inherent vulnerabilities that such components create. Component and function criticality are assessed in terms of the impact of a component or function failure on the organizational missions that are supported by the system that contains the components and functions.

Criticality analysis is performed when an architecture or design is being developed, modified, or upgraded. If such analysis is performed early in the system development life cycle, organizations may be able to modify the system design to reduce the critical nature of these components and functions, such as by adding redundancy or alternate paths into the system design. Criticality analysis can also influence the protection measures required by development contractors. In addition to criticality analysis for systems, system components, and system services, criticality analysis of information is an important consideration. Such analysis is conducted as part of security categorization in RA-2.