#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
	System and Information Integrity (SI)[1]					
1.	Does the Tribe or TGRA develop, document, and disseminate to all organizational personnel with system and information integrity responsibilities and information system owners an agency-level system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance?	____	____	____	SI-1, a.1.(a)	
	Is the agency-level system and information integrity policy consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines?	____	____	____	SI-1, a.1.(b)	
	For the questions above, simply restating controls does not constitute an organizational policy or procedure					
2.	Does the Tribe or TGRA have procedures that facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls?	____	____	____	SI-1, a.2	
3.	Based on inquiry and record examination, has the Tribe or TGRA designated organizational personnel with system and information integrity responsibilities to manage the development, documentation, and dissemination of the system, information integrity policy and procedures?	____	____	____	SI-1, b	
4.	Does the Tribe or TGRA review and update the current system and information integrity policy annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CHRI?	____	____	____	SI-1, c.1	
5.	Does the Tribe or TGRA review and update the current system and information integrity procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI?	____	____	____	SI-1, c.2	
6.	Does the Tribe or TGRA identify, report, and correct system flaws?	____	____	____	SI-2, a	

[1] These requirements are sanctionable for audit beginning October 1, 2023.

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
7.	Does the Tribe or TGRA test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation?	____	____	____	SI-2, b	
8.	Does the Tribe or TGRA install security-relevant software and firmware updates within the number of days listed after the release of the updates?					
	• Critical – 15 days	____	____	____	SI-2, c	
	• High – 30 days	____	____	____	SI-2, c	
	• Medium – 60 days	____	____	____	SI-2, c	
	• Low – 90 days; and	____	____	____	SI-2, c	
9.	Does the Tribe or TGRA incorporate flaw remediation into the organizational configuration management process?	____	____	____	SI-2, d	
10.	Based on inquiry and record examination, does the Tribe or TGRA determine if system components have applicable security-relevant software and firmware updates installed using vulnerability scanning tools at least quarterly or following any security incidents involving CJI or systems used to process, store, or transmit CJI?	____	____	____	SI-2, (2)	
11.	Based on inquiry and record examination, does the Tribe or TGRA implement signature-based malicious code protection mechanisms at system entry and exit points[2] to detect and eradicate malicious code?	____	____	____	SI-3, a	
12.	Based on inquiry and record examination, does the Tribe or TGRA automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures?	____	____	____	SI-3, b	

[2] System entry and exit points include firewalls, remote-access servers, electronic mail servers, web servers, proxy servers, workstations, notebook computers, and mobile devices.

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
13.	Based on inquiry and record examination, does the Tribe or TGRA configure malicious code protection mechanisms to perform periodic scans of the system at least daily and real-time scans of files from external sources at network entry and exit points and on all servers and endpoint devices as the files are downloaded, opened, or executed in accordance with organizational policy?	____	____	____	SI-3, c.1	
14.	Based on inquiry and record examination, does the Tribe or TGRA block or quarantine malicious code, take mitigating action(s), and when necessary, implement incident response procedures, and send alerts to system/network administrators and/or organizational personnel with information security responsibilities in response to malicious code detection?	____	____	____	SI-3, c.2	
15.	Based on inquiry and record examination, does the Tribe or TGRA address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system?	____	____	____	SI-3, d	
16.	Based on inquiry and record examination, does the Tribe or TGRA monitor the system to detect attacks and indicators of potential attacks in accordance with the following monitoring objectives:					
	a. Intrusion detection and prevention	____	____	____	SI-4, a.1.a	
	b. Malicious code protection	____	____	____	SI-4, a.1.b	
	c. Vulnerability scanning	____	____	____	SI-4, a.1.c	
	d. Audit record monitoring	____	____	____	SI-4, a.1.d	
	e. Network monitoring	____	____	____	SI-4, a.1.e	
	f. Firewall monitoring	____	____	____	SI-4, a.1.f	
17.	Based on inquiry and record examination, does the Tribe or TGRA monitor the system to detect unauthorized local, network, and remote connections?	____	____	____	SI-4, a.2	
18.	Based on inquiry and record examination, does the Tribe or TGRA identify unauthorized use of the system through the following techniques and methods: event logging (CJIS Security Policy 5.4 Audit and Accountability)?	____	____	____	SI-4, b	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
19.	Based on inquiry and record examination, does the Tribe or TGRA invoke internal monitoring capabilities or deploy monitoring devices strategically within the system to collect organization-determined essential information?	____	____	____	SI-4, c.1	
20.	Based on inquiry and record examination, does the Tribe or TGRA invoke internal monitoring capabilities or deploy monitoring devices at ad hoc locations within the system to track specific types of transactions of interest to the organization?	____	____	____	SI-4, c.2	
21.	Based on inquiry and record examination, does the Tribe or TGRA analyze detected events and anomalies?	____	____	____	SI-4, d	
22.	Based on inquiry and record examination, does the Tribe or TGRA adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the United States of America?	____	____	____	SI-4, e	
23.	Based on inquiry and record examination, does the Tribe or TGRA obtain a legal opinion regarding system monitoring activities?	____	____	____	SI-4, f	
24.	Based on inquiry and record examination, does the Tribe or TGRA provide intrusion detection and prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring, and firewall monitoring software logs weekly to organizational personnel with information security responsibilities?	____	____	____	SI-4, g	
25.	Based on inquiry and record examination, does the Tribe or TGRA employ automated tools and mechanisms to support near real-time analysis of events?	____	____	____	SI-4, (2)	
26.	Based on inquiry and record examination, does the Tribe or TGRA determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic?	____	____	____	SI-4, (4)a	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
27.	Based on inquiry and record examination, does the Tribe or TGRA monitor inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions such as: the presence of malicious code or unauthorized use of legitimate code or credentials within organizational systems or propagating among system components, signaling to external systems, and the unauthorized exporting of information?	____	____	____	SI-4, (4)b	
28.	Based on inquiry and record examination, does the Tribe or TGRA alert organizational personnel with system monitoring responsibilities when the following system-generated indications of compromise or potential compromise occur: inappropriate or unusual activities with security or privacy implications?	____	____	____	SI-4, (5)	
29.	Based on inquiry and record examination, does the Tribe or TGRA receive system security alerts, advisories, and directives from external source(s) (e.g., CISA, Multi-State Information Sharing & Analysis Center [MS-ISAC], U.S. Computer Emergency Readiness Team [USCERT], hardware/software providers, federal/state advisories, etc.) on an ongoing basis?	____	____	____	SI-5, a	
30.	Based on inquiry and record examination, does the Tribe or TGRA generate internal security alerts, advisories, and directives as deemed necessary?	____	____	____	SI-5, b	
31.	Based on inquiry and record examination, does the Tribe or TGRA disseminate security alerts, advisories, and directives to organizational personnel implementing, operating, maintaining, and using the system?	____	____	____	SI-5, c	
32.	Based on inquiry and record examination, does the Tribe or TGRA implement security directives in accordance with established time frames or notify the issuing organization of the degree of noncompliance?	____	____	____	SI-5, d	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
33.	Based on inquiry and record examination, does the Tribe or TGRA employ integrity verification tools to detect unauthorized changes to software, firmware, and information systems that contain or process CJI?	____	____	____	SI-7, a	
34.	Based on inquiry and record examination, does the Tribe or TGRA take the following actions when unauthorized changes to the software, firmware, and information are detected: notify organizational personnel responsible for software, firmware, and/or information integrity and implement incident response procedures as appropriate?	____	____	____	SI-7, b	
35.	Based on inquiry and record examination, does the Tribe or TGRA perform an integrity check of software, firmware, and information systems that contain or process CJI at agency-defined transitional states[3] or security relevant events at least weekly or in an automated fashion?	____	____	____	SI-7, (1)	
36.	Based on inquiry and record examination, does the Tribe or TGRA incorporate the detection of the following unauthorized changes into the organizational incident response capability: unauthorized changes to established configuration setting or the unauthorized elevation of system privileges?	____	____	____	SI-7, (7)	
37.	Based on inquiry and record examination, does the Tribe or TGRA employ spam protection mechanisms at system entry and exit points to detect and act on unsolicited messages?	____	____	____	SI-8, a	
38.	Based on inquiry and record examination, does the Tribe or TGRA update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures?	____	____	____	SI-8, b	
39.	Based on inquiry and record examination, does the Tribe or TGRA automatically update spam protection mechanisms at least daily?	____	____	____	SI-8, (2)	

[3] Transitional states include system startup, restart, shutdown, and abort.

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
40.	Based on inquiry and record examination, does the Tribe or TGRA check the validity of the following information inputs: all inputs to web/application servers, database servers, and any system or application input that might receive or process CJI?	____	____	____	SI-10	
41.	Based on inquiry and record examination, does the Tribe or TGRA generate error messages that provide information necessary for corrective actions without revealing information that could be exploited?	____	____	____	SI-11, a	
42.	Based on inquiry and record examination, does the Tribe or TGRA reveal error messages only to organizational personnel with information security responsibilities?	____	____	____	SI-11, b	
43.	Based on inquiry and record examination, does the Tribe or TGRA manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines and operational requirements?	____	____	____	SI-12	
44.	Based on inquiry and record examination, does the Tribe or TGRA limit personally identifiable information being processed in the information life cycle to the minimum PII necessary to achieve the purpose for which it is collected (see CJIS Security Policy Section 4.3)	____	____	____	SI-12 (1)	
45.	Based on inquiry and record examination, does the Tribe or TGRA use the following techniques to minimize the use of personally identifiable information for research, testing, or training: data obfuscation, randomization, anonymization, or use of synthetic data?	____	____	____	SI-12 (2)	
46.	Based on inquiry and record examination, does the Tribe or TGRA use the following techniques to dispose[4] of, destroy, or erase information following the retention period: as defined in MP-6?	____	____	____	SI-12 (3)	

[4] The disposal or destruction of information applies to originals as well as copies and archived records, including system logs that may contain PII.

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
47.	Based on inquiry and record examination, does the Tribe or TGRA implement the following controls to protect the system memory from unauthorized code execution: data execution prevention and address space layout randomization?	____	____	____	SI-16	