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

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
5.	Based on inquiry and record examination, has the Tribe or TGRA determined the high-level information security and privacy requirements for the system or system service in mission and business process planning?	____	____	____	SA-2, a	
6.	Based on inquiry and record examination, has the Tribe or TGRA determined, documented, and allocated the resources required to protect the system or system service as part of the organizational capital planning and investment control process?	____	____	____	SA-2, b	
7.	Based on inquiry and record examination, has the Tribe or TGRA acquired, developed, and managed the system using an agency documented system development lifecycle process that incorporates information security and privacy considerations?	____	____	____	SA-3, a	
8.	Based on inquiry and record examination, has the Tribe or TGRA defined and documented information security and privacy roles and responsibilities throughout the system development life cycle?	____	____	____	SA-3, b	
9.	Based on inquiry and record examination, has the Tribe or TGRA identified individuals having information security and privacy roles and responsibilities?	____	____	____	SA-3, c	
10.	Based on inquiry and record examination, has the Tribe or TGRA integrated the organizational information security and privacy risk management process into system development life cycle activities?	____	____	____	SA-3, d	

#	QUESTION	YES	NO	N/A	STANDARD	COMMENT
11.	Based on inquiry and record examination, has the Tribe or TGRA included the following requirements, descriptions, and criteria, explicitly or by reference, using agency defined contract language in the acquisition contract for the system, system component, or system service:					
	a. Security and privacy functional requirements?	____	____	____	SA-4, a	
	b. Strength of mechanism requirements?	____	____	____	SA-4, b	
	c. Security and privacy assurance requirements?	____	____	____	SA-4, c	
	d. Controls needed to satisfy the security and privacy requirements?	____	____	____	SA-4, d	
	e. Security and privacy documentation requirements?	____	____	____	SA-4, e	
	f. Requirements for protecting security and privacy documentation?	____	____	____	SA-4, f	
	g. Description of the system development environment and environment in which the system is intended to operate?	____	____	____	SA-4, g	
	h. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management?	____	____	____	SA-4, h	
	i. Acceptance criteria?	____	____	____	SA-4, i	
12.	Based on inquiry and record examination, does the Tribe or TGRA require the developer of the system, system component, or system service to provide a description of the functional properties of the controls to be implemented?	____	____	____	SA-4, (1)	
13.	Based on inquiry and record examination, does the Tribe or TGRA require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes: security-relevant external system interfaces; high-level design and a project plan that addresses sufficient detail to permit analysis and testing of the controls?	____	____	____	SA-4, (2)	
14.	Based on inquiry and record examination, does the Tribe or TGRA require the developer of the system, system component, or system service to identify the functions, ports, protocols, and services intended for organizational use?	____	____	____	SA-4, (9)	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
15.	Based on inquiry and record examination, does the Tribe or TGRA employ only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational systems?	____	____	____	SA-4, (10)	
16.	Based on inquiry and record examination, has the Tribe or TGRA obtained or developed administrator documentation for the system, system component, or system service that describes:					
	1. Secure configuration, installation, and operation of the system, component, or service?	____	____	____	SA-5, a.1	
	2. Effective use and maintenance of security and privacy functions and mechanisms?	____	____	____	SA-5, a.2	
	3. Known vulnerabilities regarding configuration and use of administrative or privileged functions?	____	____	____	SA-5, a.3	
17.	Based on inquiry and record examination, has the Tribe or TGRA obtained or developed user documentation for the system, system component, or system service that describes:					
	1. User-accessible security and privacy functions and mechanisms and how to effectively use those functions and mechanisms?	____	____	____	SA-5, b.1	
	2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner and protect individual privacy?	____	____	____	SA-5, b.2	
	3. User responsibilities in maintaining the security of the system, component, or service and privacy of individuals?	____	____	____	SA-5, b.3	
18.	Based on inquiry and record examination, has the Tribe or TGRA documented steps to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent by contacting manufacturers, suppliers, or developers and conducting web-based searches in response?	____	____	____	SA-5, c	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
19.	Based on inquiry and record examination, has the Tribe or TGRA distributed documentation to organizational personnel with system and services responsibilities?	____	____	____	SA-5, d	
20.	Based on inquiry and record examination, has the Tribe or TGRA applied agency documented systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components?	____	____	____	SA-8	
21.	Based on inquiry and record examination, has the Tribe or TGRA implemented the privacy principle of minimization using only the Personally Identifiable Information necessary to perform system engineering?	____	____	____	SA-8, (33)	
22.	Based on inquiry and record examination, does the Tribe or TGRA require that providers of external system services comply with organizational security and privacy requirements and employ system and services acquisition security controls in accordance with the CJISSECPOL including the following agreements when applicable: 1. Outsourcing Standards for Non-Channelers: Contractors designated to perform noncriminal justice ancillary functions on behalf of a NCJA (public) or NCJA (private) for noncriminal justice functions eligible for access to CJI. Access is permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. All contractors accessing CJI are subject to the terms and conditions described in the Compact Council Outsourcing Standard for Non-Channelers. Contractors leveraging CJI to perform civil functions on behalf of an Authorized Recipient (TGRA) must meet the same training and certification criteria required by governmental agencies performing a similar function and are subject to the same extent of audit review as are local user agencies.	____	____	____	SA-9, a.4	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
23.	Based on inquiry and record examination, has the Tribe or TGRA defined and documented organizational oversight and user roles and responsibilities with regard to external system services?	____	____	____	SA-9, b	
24.	Based on inquiry and record examination, does the Tribe or TGRA employ the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis:					
	1. All agencies having access to CJI / CHRI must permit an inspection team to conduct an appropriate inquiry and audit of any alleged security violations.	____	____	____	SA-9, c.1	
	2. At a minimum, triennially audit all external service providers which have access to the information system in order to ensure compliance with applicable statutes, regulations, and policies.	____	____	____	SA-9, c.2	
	3. Have the authority to conduct unannounced security inspections and scheduled audits of external service providers facilities?	____	____	____	SA-9, c.3	
	4. Have the authority, on behalf of another CSA (NIGC), to conduct a CJISSECPOL compliance audit of contractor facilities and provide the results to the requesting CSA (NIGC)?	____	____	____	SA-9, c.4	
	Note: Compliance audit requirements are outlined in the Security and Management Control Outsourcing Standard for Non-Channeling related to outsourcing noncriminal justice administrative functions. See the NIGC Sample Audit Checklist for Outsourcing.					
25.	Based on inquiry and record examination, does the Tribe or TGRA require providers of the following external system services to identify the functions, ports, protocols, and other services required for the use of such services: any system with a local, network, or remote connection to an agency information system?	____	____	____	SA-9, (2)	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
26.	Based on inquiry and record examination, does the Tribe or TGRA require the developer of the system, system component, or system service to:					
	a. Perform configuration management during system, component, or service during design, development, implementation, operation, and disposal?	____	____	____	SA-10, a	
	b. Document, manage, and control the integrity of changes to security configuration, network diagrams, and system components (hardware, software, firmware) by implementing access restrictions such as least privilege for changes?	____	____	____	SA-10, b	
	c. Implement only organization-approved changes to the system, component, or service?	____	____	____	SA-10, c	
	d. Document approved changes to the system, component, or service and the potential security and privacy impacts of such changes?	____	____	____	SA-10, d	
	e. Track security flaws and flaw resolution within the system, component, or service and report findings to the individual(s) with information security responsibilities and an individual(s) with system and services acquisition responsibilities?	____	____	____	SA-10, e	
27.	Based on inquiry and record examination, does the Tribe or TGRA require the developer of the system, system component, or system service, at all post-design stages of the system development life cycle, to:					
	a. Develop and implement a plan for ongoing security and privacy control assessments?	____	____	____	SA-11, a	
	b. Perform system and regression testing/evaluation at a level of comprehensive testing?	____	____	____	SA-11, b	
	c. Produce evidence of the execution of the assessment plan and the results of the testing and evaluation?	____	____	____	SA-11, c	
	d. Implement a verifiable flaw remediation process?	____	____	____	SA-11, d	
	e. Correct flaws identified during testing and evaluation?	____	____	____	SA-11, e	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
28.	Based on inquiry and record examination, does the Tribe or TGRA require the developer of the system, system component, or system service to follow a documented development process that:					
	1. Explicitly addresses security and privacy requirements?	____	____	____	SA-15, a.1	
	2. Identifies the standards and tools used in the development process?	____	____	____	SA-15, a.2	
	3. Documents the specific tool options and tool configurations used in the development process?	____	____	____	SA-15, a.3	
	4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development?	____	____	____	SA-15, a.4	
29.	Based on inquiry and record examination, has the Tribe or TGRA reviewed the development process, standards, tools, tool options, and tool configurations to determine if the process, standards, tools, tool options, and tool configurations selected and employed can satisfy security and privacy requirements during design, development, implementation, operation, and disposal?	____	____	____	SA-15, b	
30.	Based on inquiry and record examination, does the Tribe or TGRA require the developer of the system, system component, or system service to perform a criticality analysis:					
	a. At the following decision points in the system development life cycle: design, development, implementation, and operational?	____	____	____	SA-15, (1)a	
	b. At the following level of rigor: comprehensive testing?	____	____	____	SA-15, (1)b	
31.	Based on inquiry and record examination, does the Tribe or TGRA replace system components when support for the components is no longer available from the developer, vendor, or manufacturer?	____	____	____	SA-22, a	
32.	Based on inquiry and record examination, does the Tribe or TGRA provide the following options for alternative sources for continued support for unsupported components: original manufacturer support, or original contracted vendor support?	____	____	____	SA-22, b	