#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
5.10	**Systems and Communications Protection (SC)[1]**					
1.	Based on inquiry and record examination, has the Tribe or TGRA developed, documented, and disseminated to organizational personnel with system and communications protection responsibilities an agency-level system and communications protection policy that:					
	• Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance?	____	____	____	SC-1, a.1.(a)	
	• Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines?	____	____	____	SC-1, a.1.(b)	
2.	Does the Tribe or TGRA have procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls?	____	____	____	SC-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 system and communications protection policy and procedures?	____	____	____	SC-1, b	
4.	Based on inquiry and record examination, has the Tribe or TGRA reviewed and updated the current system and communications protection:					
	• Policy annually and following any changes and 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?	____	____	____	SC-1, c.1	
	• Procedures annually and following any changes and security incidents involving unauthorized access to CJI / CHRI or systems used to process, store, or transmit CJI / CHRI?	____	____	____	SC-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, does the Tribe or TGRA separate user functionality (physical or logical), including user interface services, from system management functionality[2]?	____	____	____	SC-2	
6.	Based on inquiry and record examination, does the Tribe or TGRA prevent unauthorized and unintended information transfer via shared system resources?	____	____	____	SC-4	
7.	Based on inquiry and record examination, does the Tribe or TGRA protect against or limit the effects of the following types of denial-of-service events: distributed denial of service (DDoS), Domain Name System (DNS) Denial of Service, etc?	____	____	____	SC-5, a	
8.	Based on inquiry and record examination, does the Tribe or TGRA employ the following controls to achieve the denial-of-service objective: boundary protection devices and intrusion detection or prevention devices?	____	____	____	SC-5, b	
9.	Based on inquiry and record examination, does the Tribe or TGRA monitor and control communications at the external managed interfaces[3] to the system and at key internal managed interfaces within the system?	____	____	____	SC-7, a	
10.	Based on inquiry and record examination, does the Tribe or TGRA implement subnetworks[4] for publicly accessible system components that are physically or logically separated from internal organizational networks?	____	____	____	SC-7, b	

[2] System management functionality includes functions that are necessary to administer databases, network components, workstations, or servers. These functions typically require privileged user access. The separation of user functions from system management functions is physical or logical. Organizations may separate system management functions from user functions by using different computers, instances of operating systems, central processing units, or network addresses; by employing virtualization techniques; or some combination of these or other methods. Separation of system management functions from user functions includes web administrative interfaces that employ separate authentication methods for users of any other system resources. Separation of system and user functions may include isolating administrative interfaces on different domains and with additional access controls.

[3] Managed interfaces include gateways, routers, firewalls, guards, network-based malicious code analysis, virtualization systems, or encrypted tunnels implemented within a security architecture.

[4] Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones or DMZs.

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
11.	Based on inquiry and record examination, does the Tribe or TGRA connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture?	____	____	____	SC-7, c	
12.	Based on inquiry and record examination, does the Tribe or TGRA limit the number of external network connections to the system?	____	____	____	SC-7, (3)	
13.	Based on inquiry and record examination, does the Tribe or TGRA implement a managed interface for each external telecommunication service?	____	____	____	SC-7, (4) a	
14.	Based on inquiry and record examination, does the Tribe or TGRA establish a traffic flow policy for each managed interface?	____	____	____	SC-7, (4) b	
15.	Based on inquiry and record examination, does the Tribe or TGRA protect the confidentiality and integrity of the information being transmitted across each interface?	____	____	____	SC-7, (4) c	
16.	Based on inquiry and record examination, does the Tribe or TGRA document each exception to the traffic flow policy with a supporting mission or business need and duration of that need?	____	____	____	SC-7, (4) d	
17.	Based on inquiry and record examination, does the Tribe or TGRA review exceptions to the traffic flow policy annually, after any incident, and after any major changes impacting the information system, while removing exceptions that are no longer supported by an explicit mission or business need?	____	____	____	SC-7, (4) e	
18.	Based on inquiry and record examination, does the Tribe or TGRA prevent unauthorized exchange of control plane traffic[5] with external networks?	____	____	____	SC-7, (4) f	

[5] Examples of control plane traffic include Border Gateway Protocol (BGP) routing, Domain Name System (DNS), and management protocols. See [SP 800-189] for additional information on the use of the resource public key infrastructure (RPKI) to protect BGP routes and detect unauthorized BGP announcements.

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
19.	Based on inquiry and record examination, does the Tribe or TGRA publish information to enable remote networks to detect unauthorized control plane traffic from internal networks?	____	____	____	SC-7, (4) g	
20.	Based on inquiry and record examination, does the Tribe or TGRA filter unauthorized control plane traffic from external networks?	____	____	____	SC-7, (4) h	
21.	Based on inquiry and record examination, does the Tribe or TGRA deny network communications traffic by default and allow network communications traffic by exception at boundary devices for information systems used to process, store, or transmit CJI / CHRI?[6]	____	____	____	SC-7, (5)	
22.	Based on inquiry and record examination, does the Tribe or TGRA prevent split tunneling for remote devices connecting to organizational systems?[7]	____	____	____	SC-7, (7)	

[6] Denying by default and allowing by exception applies to inbound and outbound network communications traffic. A deny-all, permit-by-exception network communications traffic policy ensures that only those system connections that are essential and approved are allowed. Deny by default, allow by exception also applies to a system that is connected to an external system.

[7] Split tunneling is the process of allowing a remote user or device to establish a non-remote connection with a system and simultaneously communicate via some other connection to a resource in an external network. This method of network access enables a user to access remote devices and simultaneously, access uncontrolled networks. Split tunneling might be desirable by remote users to communicate with local system resources, such as printers or file servers. However, split tunneling can facilitate unauthorized external connections, making the system vulnerable to attack and to exfiltration of organizational information. Split tunneling can be prevented by disabling configuration settings that allow such capability in remote devices and by preventing those configuration settings from being configurable by users. Prevention can also be achieved by the detection of split tunneling (or of configuration settings that allow split tunneling) in the remote device, and by prohibiting the connection if the remote device is using split tunneling. A virtual private network (VPN) can be used to securely provision a split tunnel. A securely provisioned VPN includes locking connectivity to exclusive, managed, and named environments, or to a specific set of pre-approved addresses, without user control.

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
23.	Based on inquiry and record examination, does the Tribe or TGRA route all internal communications traffic that may be proxied, except traffic specifically exempted by organizational personnel with information security responsibilities, to all untrusted networks through authenticated proxy servers at managed interfaces?[8]	____	____	____	SC-7, (8)	
24.	Based on inquiry and record examination, does the Tribe or TGRA for systems that process personally identifiable information (PII):					
	• Apply the following processing rules to data elements of PII: all applicable laws, executive orders, directives, regulations, policies, standards, and guidelines?	____	____	____	SC-7, (24) a	
	• Monitor for permitted processing at the external interfaces to the system and at key internal boundaries within the system?	____	____	____	SC-7, (24) b	
	• Document each processing exception?	____	____	____	SC-7, (24) c	
	• Review and remove exceptions that are no longer supported?	____	____	____	SC-7, (24) d	

[8] A proxy server is a server (i.e., system or application) that acts as an intermediary for clients requesting system resources from non-organizational or other organizational servers. System resources that may be requested include files, connections, web pages, or services. Client requests established through a connection to a proxy server are assessed to manage complexity and provide additional protection by limiting direct connectivity. Web content filtering devices are one of the most common proxy servers that provide access to the Internet. Proxy servers can support the logging of Transmission Control Protocol sessions and the blocking of specific Uniform Resource Locators, Internet Protocol addresses, and domain names. Web proxies can be configured with organization-defined lists of authorized and unauthorized websites. Note that proxy servers may inhibit the use of virtual private networks (VPNs) and create the potential for "man-in-the-middle" attacks (depending on the implementation).

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
25.	Based on inquiry and record examination, does the Tribe or TGRA protect the confidentiality and integrity of transmitted information?[9] Metadata derived from unencrypted CJI / CHRI shall be protected in the same manner as CJI / CHRI and shall not be used for any advertising or other commercial purposes by any cloud service provider or other associated entity.	____	____	____	SC-8	
26.	Based on inquiry and record examination, does the Tribe or TGRA implement cryptographic mechanisms[10] to prevent unauthorized disclosure and detect unauthorized changes or access to CJI / CHRI during transmission?	____	____	____	SC-8, (1)	
27.	Based on inquiry and record examination, does the Tribe or TGRA terminate the network connection associated with a communications session at the end of the session or after one (1) hour of inactivity?[11]	____	____	____	SC-10	

[9] Protecting the confidentiality and integrity of transmitted information applies to internal and external networks as well as any system components that can transmit information, including servers, notebook computers, desktop computers, mobile devices, printers, copiers, scanners, facsimile machines, and radios. Unprotected communication paths are exposed to the possibility of interception and modification. Protecting the confidentiality and integrity of information can be accomplished by physical or logical means. Physical protection can be achieved by using protected distribution systems. A protected distribution system is a wireline or fiber-optics telecommunications system that includes terminals and adequate electromagnetic, acoustical, electrical, and physical controls to permit its use for the unencrypted transmission of classified information. Logical protection can be achieved by employing encryption techniques. Organizations that rely on commercial providers who offer transmission services as commodity services rather than as fully dedicated services may find it difficult to obtain the necessary assurances regarding the implementation of needed controls for transmission confidentiality and integrity. In such situations, organizations determine what types of confidentiality or integrity services are available in standard, commercial telecommunications service packages. If it is not feasible to obtain the necessary controls and assurances of control effectiveness through appropriate contracting vehicles, organizations can implement appropriate compensating controls. The agency may permit limited use of metadata derived from unencrypted CJI when specifically approved by the agency and its "intended use" is detailed within the service agreement. Such authorized uses of metadata may include but are not limited to the following: spam and spyware filtering, data loss prevention, spillage reporting, transaction logs (events and content–similar to the AU controls), data usage/indexing metrics, and diagnostic/syslog data.

[10] Cryptographic mechanisms that protect the confidentiality and integrity of information during transmission include TLS and IPSec. Cryptographic mechanisms used to protect information integrity include cryptographic hash functions that have applications in digital signatures, checksums, and message authentication codes.

[11] Network disconnect applies to internal and external networks. Terminating network connections associated with specific communications sessions includes de-allocating TCP/IP address or port pairs at the operating system level and de-allocating the networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. Periods of inactivity may be established by organizations and include time periods by type of network access or for specific network accesses.

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
28.	Based on inquiry and record examination, does the Tribe or TGRA establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: encryption key generation, distribution, storage, access, and destruction is controlled by the agency?	____	____	____	SC-12	
29.	Based on inquiry and record examination, does the Tribe or TGRA determine the use of encryption for CJI / CHRI in-transit when outside a physically secure location?	____	____	____	SC-13, a	
30.	Based on inquiry and record examination, does the Tribe or TGRA implement the following types of cryptography required for each specified cryptographic use: cryptographic modules which are Federal Information Processing Standard (FIPS) 140-3 certified, or FIPS validated algorithm for symmetric key encryption and decryption (FIPS 197 [AES]), with a symmetric cipher key of at least 128-bit strength for CJI / CHRI in-transit? NOTE: Subsequent versions of approved cryptographic modules that are under current review for FIPS 140-3 compliancy can be used in the interim until certification is complete. FIPS 140-2 certificates will not be acceptable after September 21, 2026.	____	____	____	SC-13, b	
31.	Based on inquiry and record examination, does the Tribe or TGRA prohibit remote activation of collaborative computing devices and applications?[12]	____	____	____	SC-15, a	
32.	Based on inquiry and record examination, does the Tribe or TGRA provide an explicit indication of use[13] to users physically present at the devices?	____	____	____	SC-15, b	

[12] Collaborative computing devices and applications include remote meeting devices and applications, networked white boards, cameras, and microphones.

[13] The explicit indication of use includes signals to users when collaborative computing devices and applications are activated.

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
33.	Based on inquiry and record examination, does the Tribe or TGRA issue public key certificates[14] under an agency-level certificate authority or obtain public key certificates from an approved service provider?	____	____	____	SC-17, a	
34.	Based on inquiry and record examination, does the Tribe or TGRA include only approved trust anchors[15] in trust stores[16] or certificate stores managed by the organization?	____	____	____	SC-17, b	
35.	Based on inquiry and record examination, does the Tribe or TGRA define acceptable and unacceptable mobile code and mobile code technologies?[17]	____	____	____	SC-18, a	
36.	Based on inquiry and record examination, does the Tribe or TGRA authorize, monitor, and control the use of mobile code within the system?	____	____	____	SC-18, b	
37.	Based on inquiry and record examination, does the Tribe or TGRA provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries?	____	____	____	SC-20, a	
38.	Based on inquiry and record examination, does the Tribe or TGRA provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace?	____	____	____	SC-20, b	

[14] Public key infrastructure (PKI) certificates are certificates with visibility external to organizational systems and certificates related to the internal operations of systems, such as application-specific time services.
[15] A trust anchor is an authoritative source (i.e., a certificate authority) for which trust is assumed and not derived. A root certificate for a PKI system is an example of a trust anchor.
[16] A trust store or certificate store maintains a list of trusted root certificates.
[17] Mobile code includes any program, application, or content that can be transmitted across a network (e.g., embedded in an email, document, or website) and executed on a remote system. Decisions regarding the use of mobile code within organizational systems are based on the potential for the code to cause damage to the systems if used maliciously. Mobile code technologies include Java applets, JavaScript, HTML5, WebGL, and VBScript. Usage restrictions and implementation guidelines apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations and devices, including notebook computers and smart phones. Mobile code policy and procedures address specific actions taken to prevent the development, acquisition, and introduction of unacceptable mobile code within organizational systems, including requiring mobile code to be digitally signed by a trusted source.

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
39.	Based on inquiry and record examination, does the Tribe or TGRA request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources?	____	____	____	SC-21	
40.	Based on inquiry and record examination, does the Tribe or TGRA ensure the systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal and external role separation?	____	____	____	SC-22	
41.	Based on inquiry and record examination, does the Tribe or TGRA protect the authenticity of communications sessions? Protecting session authenticity addresses communications protection at the session level, not at the packet level. Such protection establishes grounds for confidence at both ends of communications sessions in the ongoing identities of other parties and the validity of transmitted information. Authenticity protection includes protecting against "man-in-the-middle" attacks, session hijacking, and the insertion of false information into sessions.	____	____	____	SC-23	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
42.	Based on inquiry and record examination, does the Tribe or TGRA protect the confidentiality and integrity of the following information at rest[18]: CJI / CHRI when outside physically secure locations using cryptographic modules which are certified FIPS 140-3 with a symmetric cipher key of at least 128-bit strength, or FIPS 197 with a symmetric cipher key of at least 256-bit strength? Metadata derived from unencrypted CJI / CHRI shall be protected in the same manner as CJI / CHRI and shall not be used for any advertising or other commercial purposes by any cloud service provider or other associated entity. The storage of CJI / CHRI, regardless of encryption status, shall only be permitted in cloud environments (e.g., government or third-party/commercial datacenters, etc.) which reside within the physical boundaries of Advisory Policy Board (APB)-member country (i.e., United States, U.S. territories, Indian Tribes, and Canada) and are under legal authority of an APB-member agency (i.e., United States–federal/state/territory, Indian Tribe, or the Royal Canadian Mounted Police).	____	____	____	SC-28	
43.	Based on inquiry and record examination, does the Tribe or TGRA implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on information systems and digital media outside physically secure locations: CJI / CHRI?	____	____	____	SC-28, (1)	

[18] Information at rest refers to the state of information when it is not in process or in transit and is located on system components. Such components include internal or external hard disk drives, storage area network devices, or databases. However, the focus of protecting information at rest is not on the type of storage device or frequency of access but rather on the state of the information. Information at rest addresses the confidentiality and integrity of information and covers user information and system information. System-related information that requires protection includes configurations or rule sets for firewalls, intrusion detection and prevention systems, filtering routers, and authentication information. Organizations may employ different mechanisms to achieve confidentiality and integrity protections, including the use of cryptographic mechanisms and file share scanning. Integrity protection can be achieved, for example, by implementing write-once-read-many (WORM) technologies. When adequate protection of information at rest cannot otherwise be achieved, organizations may employ other controls, including frequent scanning to identify malicious code at rest and secure offline storage in lieu of online storage.

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
44.	Based on inquiry and record examination, does the Tribe or TGRA maintain a separate execution domain for each executing system process? Systems can maintain separate execution domains for each executing process by assigning each process a separate address space. Each system process has a distinct address space so that communication between processes is performed in a manner controlled through the security functions, and one process cannot modify the executing code of another process. Maintaining separate execution domains for executing processes can be achieved, for example, by implementing separate address spaces. Process isolation technologies, including sandboxing or virtualization, logically separate software and firmware from other software, firmware, and data. Process isolation helps limit the access of potentially untrusted software to other system resources. The capability to maintain separate execution domains is available in commercial operating systems that employ multi-state processor technologies	____	____	____	SC-39	