For High-Impact Information Systems

FAMILY: SYSTEMS AND COMMUNICATION PROTECTION **CLASS:** TECHNICAL

SC-1 SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES - The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.

SC-1.1 - Examine system and communications protection policy and procedures; other relevant documents or records **and**

Interview organizational personnel with system and communications protection responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization develops and documents system and communications protection policy and procedures;				
(ii)	The organization disseminates system and communications protection policy and procedures to appropriate elements within the organization;				
(iii)	Responsible parties within the organization periodically review system and communications protection policy and procedures; and				
(iv)	The organization updates system and communications protection policy and procedures when organizational review indicates updates are required.				

SC-1.2 - Examine system and communications protection policy and procedures; other relevant documents or records **and**

Interview organizational personnel with system and communications protection responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The system and communications protection policy addresses				

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
	purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;				
(ii)	The system and communications protection policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and				
(iii)	The system and communications protection procedures address all areas identified in the system and communications protection policy and address achieving policy-compliant implementations of all associated security controls.				

SC-2 APPLICATION PARTITIONING - The information system separates user functionality (including user interface services) from information system management functionality.

SC-2.1 - Examine system and communications protection policy; procedures addressing application partitioning; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the information system separates user functionality (including user interface services) from information system management functionality.				

and

Test separation of user functionality from information system management functionality.

Test Steps		S	N	Findings	Initials & Date
1					

SC-3 SECURITY FUNCTION ISOLATION - The information system isolates security functions from nonsecurity functions.

SC-3.1 – Examine system and communications protection policy; procedures addressing security function isolation; list of security functions to be isolated from nonsecurity functions; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization defines the security functions of the information system to be isolated from nonsecurity functions; and				
(ii)	The information system isolates security functions from nonsecurity functions.				

and

Test separation of security functions from nonsecurity functions within the information system.

Test Steps		S	N	Findings	Initials & Date
1					

SC-4 INFORMATION REMNANCE - The information system prevents unauthorized and unintended information transfer via shared system resources.

SC-4.1 - Examine system and communications protection policy; procedures addressing information remnance; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the information system prevents unauthorized and unintended information transfer via shared system resources.				

and

Test Information system for unauthorized and unintended transfer of information via shared system resources.

	Test Steps	S	N	Findings	Initials & Date
1					

SC-5 DENIAL OF SERVICE PROTECTION - The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined list of types of denial of service attacks or reference to source for current list].

SC-5.1 - Examine system and communications protection policy; procedures addressing denial of service protection; information system design documentation; information system security plan (for list of organization-defined types of denial of service attacks to protect against or limit); information system configuration settings and associated documentation; other relevant documents or records to determine if the following requirements are met:

	Requirement	S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization defines the types of denial of service attacks (or provides references to sources of current denial of service attacks) that can be addressed by the information system; and				
(ii)	The information system protects against or limits the effects of the organization-defined or referenced types of denial of service attacks.				

and

Test the information system for protection against or limitation of the effects of denial of service attacks.

	Test Steps	S	N	Findings	Initials & Date
1					

SC-7 BOUNDARY PROTECTION - The information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.

SC-7.1 - Examine system and communications protection policy; procedures addressing boundary protection; list of key internal boundaries of the information system; information system design documentation; boundary protection hardware and software; information system configuration settings and associated documentation; other relevant documents or records, **and**

Interview selected organizational personnel with boundary protection responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization defines key internal boundaries of the information system; and				
(ii)	The information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.				

and

Test automated mechanisms implementing the access control policy for unsuccessful login attempts.

Test Steps		S	N	Findings	Initials & Date
1					

SC-7(1).1 - Examine system and communications protection policy; procedures addressing boundary protection; information system design documentation; information system hardware and software; information system architecture; information system configuration settings and associated documentation; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the organization physically allocates publicly accessible information system components to separate sub-networks with separate, physical network interfaces.				

SC-7(2).1 - Examine system and communications protection policy; procedures addressing boundary protection; list of mediation vehicles for allowing public access to the organization's internal networks; information system design documentation; boundary

protection hardware and software; information system configuration settings and associated documentation; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization defines the mediation necessary for public access to the organization's internal networks; and				
(ii)	The organization prevents public access into the organization's internal networks except as appropriately mediated.				

SC-7(3).1 - Examine system and communications protection policy; procedures addressing boundary protection; information system design documentation; boundary protection hardware and software; information system architecture and configuration documentation; information system configuration settings and associated documentation; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the organization limits the number of access points to the information system to allow for better monitoring of inbound and outbound network traffic.				

SC-7(4).1 - Examine system and communications protection policy; procedures addressing boundary protection; information system security architecture; information system design documentation; boundary protection hardware and software; information system architecture and configuration documentation; information system configuration settings and associated documentation; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization defines the security controls (i.e. boundary protection devices and architectural configuration of the devices) appropriate at each external interface to a telecommunication service; and				
(ii)	The organization implements a managed interface with any external telecommunication service, implementing controls appropriate to the				

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
	required protection of the confidentiality and integrity of the information being transmitted.				

SC-7(5).1 - Examine system and communications protection policy; procedures addressing boundary protection; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the information system denies network traffic by default and allows network traffic by exception.				

SC-8 TRANSMISSION INTEGRITY - The information system protects the integrity of transmitted information.

SC-8.1 - Examine system and communications protection policy; procedures addressing transmission integrity; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the information system protects the integrity of transmitted information.				

and

Test transmission integrity capability within the information system.

Test Steps		S	N	Findings	Initials & Date
1					

SC-9 TRANSMISSION CONFIDENTIALITY - The information system protects the confidentiality of transmitted information.

SC-9.1 - Examine system and communications protection policy; procedures addressing transmission confidentiality; information system design documentation; contracts for telecommunications services; information system configuration settings and associated documentation; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the information system protects the confidentiality of transmitted information.				

and

Test transmission confidentiality capability within the information system.

Test Steps		S	N	Findings	Initials & Date
1					

SC-10 NETWORK DISCONNECT - The information system terminates a network connection at the end of a session or after [Assignment: organization-defined time period] of inactivity.

SC-10.1 - Examine system and communications protection policy; procedures addressing network disconnect; information system design documentation; organization-defined time period of inactivity before network disconnect; information system configuration settings and associated documentation; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization defines the time period of inactivity before the information system terminates a network connection; and				
(ii)	The information system terminates a network connection at the end of a session or after the organization-defined time period of inactivity.				

and

Test network disconnect capability within the information system to determine if the following requirements are met:

	Test Steps	S	N	Findings	Initials & Date
1	Test the network disconnection capability for the information system by leaving an open session for a specified amount of time to determine if the system terminates the network connection as expected				

SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT - When cryptography is required and employed within the information system, the organization establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures.

SC-12.1 - Examine system and communications protection policy; procedures addressing cryptographic key management and establishment; NIST Special Publications 800-56 and 800-57; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records **and**

Interview organizational personnel with responsibilities for cryptographic key establishment or management to determine if the following requirements are met:

	Requirement	S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the organization establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures, when cryptography is required and employed within the information system.				

and

Test automated mechanisms implementing cryptographic key management and establishment within the information system.

	Test Steps	S	N	Findings	Initials & Date
1					

SC-13 USE OF CRYPTOGRAPHY - For information requiring cryptographic protection, the information system implements cryptographic mechanisms that comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

SC-13.1 - Examine system and communications protection policy; procedures addressing use of cryptography; FIPS 140-2 (as amended); NIST Special Publications 800-56 and 800-57; information system design documentation; information system configuration settings and associated documentation; cryptographic module validation certificates; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if, for information requiring cryptographic protection, the information system implements cryptographic mechanisms that comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.				

SC-14 PUBLIC ACCESS PROTECTIONS - The information system protects the integrity and availability of publicly available information and applications.

SC-14.1 - Examine system and communications protection policy; procedures addressing public access protections; access control policy and procedures; boundary protection procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the information system protects the integrity and availability of publicly available information and applications.				

and

Test automated mechanisms implementing access controls and boundary protection for publicly available information and applications within the information system.

Test Steps		S	N	Findings	Initials & Date
1					

SC-15 COLLABORATIVE COMPUTING - The information system prohibits remote activation of collaborative computing mechanisms and provides an explicit indication of use to the local users.

SC-15.1 - Examine system and communications protection policy; procedures addressing collaborative computing; access control policy and procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the information system prohibits remote activation of collaborative computing mechanisms and provides an explicit indication of use to the local users.				

and

Test automated mechanisms implementing access controls for collaborative computing environments; alert notification for local users.

Test Steps		S	N	Findings	Initials & Date
1					

SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES - The organization issues public key certificates under an appropriate certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider.

SC-17.1 - Examine system and communications protection policy; procedures addressing public key infrastructure certificates; public key certificate policy or policies; public key issuing process; NIST Special Publication 800-32; other relevant documents or records **and**

Interview organizational personnel with public key infrastructure certificate issuing responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the organization issues public key certificates under an appropriate certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider.				

SC-18 MOBILE CODE - The organization: (i) establishes usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously; and (ii) authorizes, monitors, and controls the use of mobile code within the information system.

SC-18.1 - Examine system and communications protection policy; procedures addressing mobile code; mobile code usage restrictions, mobile code implementation guidance; NIST Special Publication 800-28; other relevant documents or records

and

Interview organizational personnel with mobile code authorization, monitoring control responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization establishes usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously; and				
(ii)	The organization authorizes, monitors, and controls the use of mobile code within the information system.				

and

Test mobile code authorization and monitoring capability for the organization.

Test Steps		S	N	Findings	Initials & Date
1					

SC-19 VOICE OVER INTERNET PROTOCOL - The organization: (i) establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and (ii) authorizes, monitors, and controls the use of VoIP within the information system.

SC-19.1 - Examine system and communications protection policy; procedures addressing VoIP; NIST Special Publication 800-58; VoIP usage restrictions; other relevant documents or records **and**

Inerview organizational personnel with VoIP authorization and monitoring responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization establishes usage restrictions and implementation guidance for Voice over Internet Protocol technologies based on the potential to cause damage to the information system if used maliciously; and				
(ii)	The organization authorizes, monitors, and controls the use of VoIP within the \information system.				

SC-20 SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) - The information system that provides name/address resolution service provides additional data origin and integrity artifacts along with the authoritative data it returns in response to resolution queries.

SC-20.1 - Examine system and communications protection policy; procedures addressing secure name/address resolution service (authoritative source); NIST Special Publication 800-81; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the information system that provides the name/address lookup service for accessing organizational information resources to entities across the Internet provides artifacts for additional data origin authentication and data integrity artifacts along with the authoritative data it returns in response to resolution queries.				

and

Test automated mechanisms implementing secure name/address resolution service (authoritative source) within the information system.

Test Steps		S	N	Findings	Initials & Date
1					

SC-21 SECURE NAME/ADDRESS RESOLUTION SERVICE (RECURSIVE OR CHACHING RESOLVER) - The information system that provides name/address resolution service for local clients performs data origin authentication and data integrity verification on the resolution responses it receives from authoritative sources when requested by client systems.

SC-21.1 – Examine system and communications protection policy; procedures addressing secure name/address resolution service (recursive or caching resolver); information system design documentation; information system configuration settings and associated documentation; other relevant documents or records to determine if the following requirements are met:.

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the information system that provides name/address resolution service for local clients performs data origin authentication and data integrity verification on the resolution responses it receives from authoritative sources when requested by client systems.				

and

Test automated mechanisms supporting name/address resolution service for fault tolerance and role separation.

Test Steps		S	N	Findings	Initials & Date
1					

SC-22 ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE - The information systems that collectively provide name/address resolution service for an organization are fault tolerant and implement role separation.

SC-22.1 - Examine system and communications protection policy; procedures addressing secure name/address resolution service (recursive or caching resolver); access control policy and procedures; NIST Special Publication 800-81; information system design documentation; assessment results from independent, testing organizations; information system configuration settings and associated documentation; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the information systems that collectively provide name/address resolution service for an organization are fault tolerant				

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
	and implement role separation.				

and

Test automated mechanisms implementing data origin authentication and integrity verification for resolution services within the information system.

Test Steps		S	N	Findings	Initials & Date
1					

SC-23 SESSION AUTHENTICITY - The information system provides mechanisms to protect the authenticity of communications sessions.

SC-23.1 - Examine system and communications protection policy; procedures addressing session authenticity; NIST Special Publications 800-52, 800-77, and 800-95; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the information system provides mechanisms to protect the authenticity of communications sessions.				

and

Test automated mechanisms implementing session authenticity.

Test Steps		S	N	Findings	Initials & Date
1					