For High-Impact Information Systems

FAMILY: SYSTEMS AND SERVICES ACQUISITION **CLASS:** MANAGEMENT

SA-1 SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES - The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and services acquisition policy that includes information security considerations and 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 services acquisition policy and associated system and services acquisition controls.

SA-1.1 - Examine system and services acquisition policy and procedures; other relevant documents or records **and**

Interview organizational personnel with system and services acquisition responsibilities to determine if the follow requirements are met:

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

SA-1.2 - Examine system and services acquisition policy and procedures; other relevant documents or records **and**

Interview organizational personnel with system and services acquisition responsibilities to determine if the follow requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The system and services acquisition policy addresses purpose, scope, roles and responsibilities, management commitment,				

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

SA-2 ALLOCATION OF RESOURCES - The organization determines, documents, and allocates as part of its capital planning and investment control process, the resources required to adequately protect the information system.

SA-2.1 - Examine system and services acquisition policy; procedures addressing the allocation of resources to information security requirements; NIST Special Publication 800-65; other relevant documents or records **and**

Interview organizational personnel with capital planning and investment responsibilities to determine if the follow requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization determines, documents, and allocates as part of its capital planning and investment control process, the resources required to adequately protect the information system.				
(ii)	The organization determines security requirements for the information system in mission/business case planning.				
(iii)	The organization establishes a discrete line item for information system security in the organization's programming and budgeting documentation.				
(iv)	The organization's programming and budgeting process is consistent with NIST Special Publication 800-65.				

SA-3 LIFE CYCLE SUPPORT - The organization manages the information system using a system development life cycle methodology that includes information security considerations.

SA-3.1 - Examine system and services acquisition policy; procedures addressing the integration of information security into the system development life cycle process; NIST Special Publication 800-64; information system development life cycle documentation; other relevant documents or records **and**

Interview organizational personnel with information security and system life cycle development responsibilities to determine if the follow requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization manages the information system using a system development life cycle methodology that includes information security considerations.				
(ii)	The organization uses a system development life cycle that is consistent with NIST Special Publication 800-64.				

SA-4 ACQUISITIONS - The organization includes security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable laws, Executive Orders, directives, policies, regulations, and standards.

SA-4.1 - Examine system and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; NIST Special Publications 800-23 and 800-70; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records **and**

Interview organizational personnel with information system security, acquisition and contracting responsibilities to determine if the follow requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization includes security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable laws, Executive Orders, directives, policies, regulations, and standards.				
(ii)	The organization's acquisition of commercial information technology products is consistent with NIST Special Publication 800-23.				
(iii)	References to security configuration settings and security				

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
	implementation guidance in organizational acquisitions are consistent with NIST Special Publication 800-70.				
(iv)	Acquisition contracts for information systems include, either explicitly or by reference, security requirements and/or security specifications that describe: - required security capabilities; - required design and development processes; - required test and evaluation procedures; and - required documentation.				

SA-4(1).1 - Examine system and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records, **and**

Interview organizational personnel with information system security, acquisition, and contracting 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 requires in solicitation documents that appropriate documentation be provided describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.				

SA-5 INFORMATION SYSTEM DOCUMENTATION - The organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system.

SA-5.1 - Examine system and services acquisition policy; procedures addressing the requirements for information system documentation; information system documentation including administrator and user guides; other relevant documents or records responsibilities

and

Interview organizational personnel with information system documentation responsibilities; organizational personnel operating, using, and/or maintaining the information system to determine if the follow requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system.				
(ii)	The organization makes available information on configuring, installing, and operating the information system.				
(iii)	The organization makes available information on effectively using the security features in the information system.				

SA-5(1).1 - Examine system and services acquisition policy; procedures addressing the requirements for information system documentation; information system design documentation; other relevant documents or records, **and**

Interview organizational personnel with information system security, acquisition, and contracting responsibilities; organizational personnel operating, using, and/or maintaining the information system 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 includes, in addition to administrator and user guides, documentation, if available from the vendor/manufacturer, describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.				

SA-6 SOFTWARE USAGE RESTRICTIONS - The organization complies with software usage restrictions.

SA-6.1 - Examine system and services acquisition policy; procedures addressing software usage restrictions; site license documentation; list of software usage restrictions; other relevant documents or records **and**

Interview organizational personnel with information system administration responsibilities; organizational personnel operating, using, and/or maintaining the information system to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization complies with software usage restrictions.				
(ii)	The organization regularly reviews/analyzes software usage for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.				

SA-7 USER INSTALLED SOFTWARE - The organization enforces explicit rules governing the installation of software by users.

SA-7.1 - Examine system and services acquisition policy; procedures addressing user installed software; list of rules governing user installed software; network traffic on the information system; other relevant documents or records, **and**

Interview organizational personnel with information system administration responsibilities; organizational personnel operating, using, and/or maintaining the information system to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization enforces explicit rules governing the installation of software by users.				
(ii)	Unauthorized software is present on the system.				
(iii)	The organization regularly reviews/analyzes user installed software for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary action.				

and

Test enforcement of rules for user installed software on the information system; information system for prohibited software.

SA-8 SECURITY ENGINEERING PRINCIPLES - The organization designs and implements the information system using security engineering principles.

SA-8.1 - Examine system and services acquisition policy; procedures addressing security engineering principles used in the development and implementation of the information system; NIST Special Publication 800-27; information system design documentation; security requirements and security specifications for the information system; other relevant documents or records

and

Interview organizational personnel with system and services acquisition 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 designs and implements the information system using security engineering principles.				
(ii)	The organization considers security design principles in the development and implementation of the information system consistent with NIST Special Publication 800-27.				

SA-9 EXTERNAL INFORMATION SYSTEM SERVICES - The organization: (i) requires that providers of external information system services employ adequate security controls in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, guidance, and established service-level agreements; and (ii) monitors security control compliance.

SA-9.1 - Examine system and services acquisition policy; procedures addressing external information system services; acquisition contracts and service level agreements; organizational security requirements and security specifications for external provider services; security control assessment evidence from external providers of information system services; other relevant documents or records

and

Interview organizational personnel with system and services acquisition responsibilities; external providers of information system services to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization requires that providers of external information system services employ adequate security controls in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, guidance, and established service-level agreements.				

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(ii)	The organization monitors security control compliance.				
(iii)	The organization regularly reviews/analyzes outsourced information system services for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.				
(iv)	The security controls employed by providers of external information system services are compliant with applicable federal laws, directives, policies, regulations, standards, guidance, and established service level agreements.				

SA-10 DEVELOPER CONFIGURATION MANAGEMENT - The organization requires that information system developers create and implement a configuration management plan that controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and its implementation.

SA-10.1 - Examine system and services acquisition policy; procedures addressing information system developer/integrator configuration management; acquisition contracts and service level agreements; information system developer/integrator configuration management plans; security flaw tracking records; system change authorization records; 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 requires that information system developers (and systems integrators) create and implement a configuration management plan that controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and its implementation.				

SA-11 DEVELOPER SECURITY TESTING - The organization requires that information system developers create a security test and evaluation plan, implement the plan, and document the results.

SA-11.1 - Examine system and services acquisition policy; procedures addressing information system developer/integrator security testing; acquisition contracts and service level agreements; information system developer/integrator security test plans; records of

developer/integrator security testing results for the information system; 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 requires that information system developers (and systems integrators) create a security test and evaluation plan, implement the plan, and document the results.				