

Department of the Interior
Security Control Standard
System and Service Acquisition

April 2011

Version: 1.1



Signature Approval Page

Designated Official	
Bernard J. Mazer, Department of the Interior, Chief Information Officer	
Signature:	Date:

REVISION HISTORY

Author	Version	Revision Date	Revision Summary
Chris Peterson	0.1	January 28, 2011	Initial draft
Timothy Brown	0.2	January 31, 2011	Incorporated comments into body text
Timothy Brown	1.0	February 17, 2011	Final review and version change to 1.0
Lawrence K. Ruffin	1.1	April 29, 2011	Final revisions and version change to 1.1

TABLE OF CONTENTS

REVISION HISTORY	3
TABLE OF CONTENTS	4
SECURITY CONTROL STANDARD: SYSTEM AND SERVICES AQUISITION	5
SA-1 SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES	5
SA-2 ALLOCATION OF RESOURCES	6
SA-3 LIFE CYCLE SUPPORT	6
SA-4 AQUISITIONS	7
SA-5 INFORMATION SYSTEM DOCUMENTATION	8
SA-6 SOFTWARE USAGE RESTRICTIONS	9
SA-7 USER INSTALLED SOFTWARE	9
SA-8 SECURITY ENGINEERING PRINCIPLES	10
SA-9 EXTERNAL INFORMATION SYSTEM SERVICES	10
SA-10 DEVELOPER CONFIGURATION MANAGEMENT	11
SA-11 DEVELOPER SECURITY TESTING	12
SA-12 SUPPLY CHAIN PROTECTION	13
SA-13 TRUSTWORTHINESS	13

SECURITY CONTROL STANDARD: SYSTEM AND SERVICES ACQUISITION

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 describes the required process for selecting and specifying security controls for an information system based on its security categorizing, including tailoring the initial set of baseline security controls and supplementing the tailored baseline as necessary based on an organizational assessment of risk.

This standard specifies organization-defined parameters that are deemed necessary or appropriate to achieve a consistent security posture across the Department of the Interior. In addition to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 System and Services Acquisition (SA) control family standard, supplemental information is included that establishes an enterprise-wide standard for specific controls within the control family. In some cases additional agency-specific or Office of Management and Budget (OMB) requirements have been incorporated into relevant controls. Where the NIST SP 800-53 indicates the need for organization-defined parameters or selection of operations that are not specified in this supplemental standard, the System Owner shall appropriately define and document the parameters based on the individual requirements, purpose, and function of the information system. The supplemental information provided in this standard is required to be applied when the Authorizing Official (AO) has selected the control, or control enhancement, in a manner that is consistent with the Department's IT security policy and associated information security Risk Management Framework (RMF) strategy.

Additionally, information systems implemented within cloud computing environments shall select, implement, and comply with any additional and/or more stringent security control requirements as specified and approved by the Federal Risk and Authorization Management Program (FedRAMP) unless otherwise approved for risk acceptance by the AO. The additional controls required for implementation within cloud computing environments are readily identified within the Priority and Baseline Allocation table following each control and distinguished by the control or control enhancement represented in **bold red text**.

SA-1 SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES

Applicability: Bureaus and Offices

Control: The organization develops, disseminates, and reviews/updates at least annually:

- a. 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
- b. Formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the system and services acquisition family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational

policies and procedures may make the need for additional specific policies and procedures unnecessary. The system and services acquisition policy can be included as part of the general information security policy for the organization. System and services acquisition procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the system and services acquisition policy. Related control: PM- 9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100

Priority and Baseline Allocation:

P1	LOW SA-1	MOD SA-1	HIGH SA-1
-----------	-----------------	-----------------	------------------

SA-2 ALLOCATION OF RESOURCES

Applicability: All Information Systems

Control: The organization:

- a. Includes a determination of information security requirements for the information system in mission/business process planning;
- b. Determines, documents, and allocates the resources required to protect the information system as part of its capital planning and investment control process; and
- c. Establishes a discrete line item for information security in organizational programming and budgeting documentation.

Supplemental Guidance: Related controls: PM-3, PM-11.

Control Enhancements: None.

References: NIST Special Publication 800-65.

Priority and Baseline Allocation:

P1	LOW SA-2	MOD SA-2	HIGH SA-2
-----------	-----------------	-----------------	------------------

SA-3 LIFE CYCLE SUPPORT

Applicability: All Information Systems

Control: The organization:

- a. Manages the information system using a system development life cycle methodology that includes information security considerations ;
- b. Defines and documents information system security roles and responsibilities throughout the system development life cycle; and
- c. Identifies individuals having information system security roles and responsibilities.

Supplemental Guidance: Related control: PM-7.

Control Enhancements: None.

References: NIST Special Publication 800-64.

Priority and Baseline Allocation:

P1	LOW SA-3	MOD SA-3	HIGH SA-3
-----------	-----------------	-----------------	------------------

SA-4 ACQUISITIONS

Applicability: All Information Systems

Control: The organization includes the following requirements and/or specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards:

- a. Security functional requirements/specifications;
- b. Security-related documentation requirements; and
- c. Developmental and evaluation-related assurance requirements.

Supplemental Guidance: The acquisition documents for information systems, information system components, and information system services include, either explicitly or by reference, security requirements that describe: (i) required security capabilities (i.e., security needs and, as necessary, specific security controls and other specific FISMA requirements); (ii) required design and development processes; (iii) required test and evaluation procedures; and (iv) required documentation. The requirements in the acquisition documents permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented. Acquisition documents also include requirements for appropriate information system documentation. The documentation addresses user and system administrator guidance and information regarding the implementation of the security controls in the information system. The level of detail required in the documentation is based on the security categorization for the information system. In addition, the required documentation includes security configuration settings and security implementation guidance. FISMA reporting instructions provide guidance on configuration requirements for federal information systems.

Control Enhancements:

1. The organization requires in acquisition documents that vendors/contractors provide information describing the functional properties of the security controls to be employed within the information system, information system components, or information system services in sufficient detail to permit analysis and testing of the controls.
2. The organization requires in acquisition documents that vendors/contractors provide information describing the design and implementation details of the security controls to be employed within the information system, information system components, or information system services (including functional interfaces among control components) in sufficient detail to permit analysis and testing of the controls.
4. The organization ensures that each information system component acquired is explicitly assigned to an information system, and that the owner of the system acknowledges this assignment.

7. The organization:
- a. Limits the use of commercially provided information technology products to those products that have been successfully evaluated against a validated U.S. Government Protection Profile for a specific technology type, if such a profile exists; and
 - b. Requires, if no U.S. Government Protection Profile exists for a specific technology type but a commercially provided information technology product relies on cryptographic functionality to enforce its security policy, then the cryptographic module is FIPS-validated.

References: ISO/IEC 15408; FIPS 140-2; NIST Special Publications 800-23, 800-35, 800-36, 800-64, 800-70; Web: WWW.NIAP-CCEVS.ORG.

Priority and Baseline Allocation:

P1	LOW SA-4	MOD SA-4 (1) (4) (7)	HIGH SA-4 (1) (2) (4) (7)
-----------	-----------------	-----------------------------	----------------------------------

SA-5 INFORMATION SYSTEM DOCUMENTATION

Applicability: All Information Systems

Control: The organization:

- a. Obtains, protects as required, and makes available to authorized personnel, administrator documentation for the information system that describes:
 - Secure configuration, installation, and operation of the information system;
 - Effective use and maintenance of security features/functions; and
 - Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; and
- b. Obtains, protects as required, and makes available to authorized personnel, user documentation for the information system that describes:
 - User-accessible security features/functions and how to effectively use those security features/functions;
 - Methods for user interaction with the information system, which enables individuals to use the system in a more secure manner; and
 - User responsibilities in maintaining the security of the information and information system; and
- c. Documents attempts to obtain information system documentation when such documentation is either unavailable or nonexistent.

Supplemental Guidance: The inability of the organization to obtain necessary information system documentation may occur, for example, due to the age of the system and/or lack of support from the vendor/contractor. In those situations, organizations may need to recreate selected information system documentation if such documentation is essential to the effective implementation and/or operation of security controls.

Control Enhancements:

1. The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacture documentation that describes the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing.
2. The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacture documentation that describes the security-relevant external interfaces to the information system with sufficient detail to permit analysis and testing.
3. The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacture documentation that describes the high-level design of the information system in terms of subsystems and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing.

Enhancement Supplemental Guidance: An information system can be partitioned into multiple subsystems.

References: None.

Priority and Baseline Allocation:

P2	LOW SA-5	MOD SA-5 (1) (3)	HIGH SA-5 (1) (2) (3)
-----------	-----------------	-------------------------	------------------------------

SA-6 SOFTWARE USAGE RESTRICTIONS

Applicability: All Information Systems

Control: The organization:

- a. Uses software and associated documentation in accordance with contract agreements and copyright laws;
- b. Employs tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution; and
- c. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

Supplemental Guidance: Tracking systems can include, for example, simple spreadsheets or fully automated, specialized applications depending on the needs of the organization.

Control Enhancements: None Mandated.

References: None.

Priority and Baseline Allocation:

P1	LOW SA-6	MOD SA-6	HIGH SA-6
-----------	-----------------	-----------------	------------------

SA-7 USER INSTALLED SOFTWARE

Applicability: All Information Systems

Control: The organization enforces explicit rules governing the installation of software by users.

Supplemental Guidance: If provided the necessary privileges, users have the ability to install software. The organization identifies what types of software installations are permitted (e.g., updates and security patches to existing software) and what types of installations are prohibited (e.g., software whose pedigree with regard to being potentially malicious is unknown or suspect). Related control: CM-2.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	LOW SA-7	MOD SA-7	HIGH SA-7
-----------	-----------------	-----------------	------------------

SA-8 SECURITY ENGINEERING PRINCIPLES

Applicability: Moderate and High Impact Information Systems

Control: The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

Supplemental Guidance: The application of security engineering principles is primarily targeted at new development information systems or systems undergoing major upgrades and is integrated into the system development life cycle. For legacy information systems, the organization applies security engineering principles to system upgrades and modifications to the extent feasible, given the current state of the hardware, software, and firmware within the system. Examples of security engineering principles include, for example: (i) developing layered protections; (ii) establishing sound security policy, architecture, and controls as the foundation for design; (iii) incorporating security into the system development life cycle; (iv) delineating physical and logical security boundaries; (v) ensuring system developers and integrators are trained on how to develop secure software; (vi) tailoring security controls to meet organizational and operational needs; and (vii) reducing risk to acceptable levels, thus enabling informed risk management decisions.

Control Enhancements: None.

References: NIST Special Publication 800-27.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD SA-8	HIGH SA-8
-----------	-------------------------	-----------------	------------------

SA-9 EXTERNAL INFORMATION SYSTEM SERVICES

Applicability: All Information Systems

Control: The organization:

- a. Requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
- b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and
- c. Monitors security control compliance by external service providers.

Supplemental Guidance: An external information system service is a service that is implemented outside of the authorization boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system). Relationships with external service providers are established in a variety of ways, for example, through joint ventures, business partnerships, outsourcing arrangements (i.e., contracts, interagency agreements, lines of business arrangements), licensing agreements, and/or supply chain exchanges. The responsibility for adequately mitigating risks arising from the use of external information system services remains with the authorizing official. Authorizing officials require that an appropriate chain of trust be established with external service providers when dealing with the many issues associated with information security. For services external to the organization, a chain of trust requires that the organization establish and retain a level of confidence that each participating provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered to the organization. The extent and nature of this chain of trust varies based on the relationship between the organization and the external provider. Where a sufficient level of trust cannot be established in the external services and/or service providers, the organization employs compensating security controls or accepts the greater degree of risk. The external information system services documentation includes government, service provider, and end user security roles and responsibilities, and any service-level agreements. Service-level agreements define the expectations of performance for each required security control, describe measurable outcomes, and identify remedies and response requirements for any identified instance of noncompliance.

Control Enhancements:

- 1. The organization:
 - a. Conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services; and
 - b. Ensures that the acquisition or outsourcing of dedicated information security services is approved by [Assignment: organization-defined senior organizational official].

Enhancement Supplemental Guidance: Dedicated information security services include, for example, incident monitoring, analysis and response, operation of information security-related devices such as firewalls, or key management services.

References: NIST Special Publication 800-35.

Priority and Baseline Allocation:

P1	LOW SA-9	MOD SA-9 (1)	HIGH SA-9 (1)
-----------	-----------------	---------------------	----------------------

SA-10 DEVELOPER CONFIGURATION MANAGEMENT

Applicability: Moderate and High Impact Information Systems

Control: The organization requires that information system developers/integrators:

- a. Perform configuration management during information system design, development, implementation, and operation;
- b. Manage and control changes to the information system;
- c. Implement only organization-approved changes;
- d. Document approved changes to the information system; and
- e. Track security flaws and flaw resolution.

Supplemental Guidance: Related controls: CM-3, CM-4, CM-9.

Control Enhancements: None Mandated.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD SA-10	HIGH SA-10
-----------	-------------------------	------------------	-------------------

SA-11 DEVELOPER SECURITY TESTING

Applicability: Moderate and High Impact Information Systems

Control: The organization requires that information system developers/integrators, in consultation with associated security personnel (including security engineers):

- a. Create and implement a security test and evaluation plan;
- b. Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and
- c. Document the results of the security testing/evaluation and flaw remediation processes.

Supplemental Guidance: Developmental security test results are used to the greatest extent feasible after verification of the results and recognizing that these results are impacted whenever there have been security-relevant modifications to the information system subsequent to developer testing. Test results may be used in support of the security authorization process for the delivered information system.

Related control: CA-2, SI-2.

Control Enhancements:

1. The organization requires that information system developers/integrators employ code analysis tools to examine software for common flaws and document the results of the analysis.

References: None.

Priority and Baseline Allocation:

P2	LOW Not Selected	MOD SA-11 (1)	HIGH SA-11(1)
-----------	-------------------------	----------------------	----------------------

SA-12 SUPPLY CHAIN PROTECTION

Applicability: Moderate and High Impact Information Systems

Control: The organization requires that information system developers/integrators, in consultation with associated security personnel (including security engineers):

- d. Create and implement a security test and evaluation plan;
- e. implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and
- f. Document the results of the security testing/evaluation and flaw remediation processes.

Supplemental Guidance: Developmental security test results are used to the greatest extent feasible after verification of the results and recognizing that these results are impacted whenever there have been security-relevant modifications to the information system subsequent to developer testing. Test results may be used in support of the security authorization process for the delivered information system.

Related control: CA-2, SI-2.

Control Enhancements: None Mandated.

References: None.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD SA-12	HIGH SA-12
----	------------------	-----------	------------

SA-13 TRUSTWORTHINESS

Applicability: High Impact Information Systems

Control: The organization requires that the information system meets **[Assignment: organization-defined level of trustworthiness]**.

Supplemental Guidance: The intent of this control is to ensure that organizations recognize the importance of trustworthiness and making explicit trustworthiness decisions when designing, developing, and implementing organizational information systems. Trustworthiness is a characteristic or property of an information system that expresses the degree to which the system can be expected to preserve the confidentiality, integrity, and availability of the information being processed, stored, or transmitted by the system. Trustworthy information systems are systems that are capable of being trusted to operate within defined levels of *risk* despite the environmental disruptions, human errors, and purposeful attacks that are expected to occur in the specified environments of operation. Two factors affecting the trustworthiness of an information system include: (i) *security functionality* (i.e., the security features or functions employed within the system); and (ii) *security assurance* (i.e., the grounds for confidence that the security functionality is effective in its application).

Appropriate security functionality for the information system can be obtained by using the Risk Management Framework (Steps 1, 2, and 3) to select and implement the necessary management, operational, and technical security controls necessary to mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation. Appropriate security assurance can be obtained

by: (i) the actions taken by developers and implementers of security controls with regard to the design, development, implementation, and operation of those controls; and (ii) the actions taken by assessors to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system.

Developers and implementers can increase the assurance in security controls by employing well-defined security policy models, structured, disciplined, and rigorous hardware and software development techniques, and sound system/security engineering principles. Assurance is also based on the assessment of evidence produced during the initiation, acquisition/development, implementation, and operations/maintenance phases of the system development life cycle. For example, developmental evidence may include the techniques and methods used to design and develop security functionality. Operational evidence may include flaw reporting and remediation, the results of security incident reporting, and the results of the ongoing monitoring of security controls. Independent assessments by qualified assessors may include analyses of the evidence as well as testing, inspections, and audits. Minimum assurance requirements are described in Appendix E.

Explicit trustworthiness decisions highlight situations where achieving the information system resilience and security capability necessary to withstand cyber attacks from adversaries with certain threat capabilities may require adjusting the risk management strategy, the design of mission/business processes with regard to automation, the selection and implementation rigor of management and operational protections, or the selection of information technology components with higher levels of trustworthiness. Trustworthiness may be defined on a component-by-component, subsystem-by-subsystem, or function-by-function basis. It is noted, however, that typically functions, subsystems, and components are highly interrelated, making separation by trustworthiness perhaps problematic and at a minimum, something that likely requires careful attention in order to achieve practically useful results. Related controls: RA-2, SA-4, SA-8, SC-3.

Control Enhancements: None Mandated.

References: FIPS Publications 199, 200; NIST Special Publications 800-53, 800-53A, 800-60, 800-64.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD Not Selected	HIGH SA-13
-----------	-------------------------	-------------------------	-------------------