Information Security – System and Services Acquisition (SA) Procedure

Directive No: CIO 2150.3-P-15.2

Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19

Information Security – System and Services Acquisition (SA) Procedure

1. PURPOSE

The Environmental Protection Agency (EPA) is responsible for ensuring all offices within the Agency meet the minimum-security requirements defined in the Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*. All EPA information systems shall meet the security requirements by implementing the security controls defined in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*.

The purpose of this procedure is to facilitate the implementation of the EPA security control requirements for the System and Services Acquisition (SA) control family, as identified in NIST SP 800-53, Revision 5.

2. SCOPE

These procedures address all EPA information and information systems to include information and information systems used, managed or operated by a contractor, another agency or other organization on behalf of the EPA.

3. AUDIENCE

Senior Information Officials (SIO), Information Security Officers (ISO) and EPA System Owners (SO) or their official designees, for EPA-operated systems, and Service Managers (SM), for systems operated on behalf of the EPA, EPA employees, contractors and all other users of EPA information and systems.

4. AUTHORITY

- Federal Information Security Modernization Act (FISMA) of 2014, Public Law 113-283, to amend chapter 35 of title 44, United States Code (U.S.C.)
- Office of Management and Budget (OMB) Circular A-130, “Managing Information as a Strategic Resource,” July 2016
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006
- NIST SP 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations, September 2020
- NIST SP 800-53B, Control Baselines for Information Systems and Organizations, October 2020
- 32 CFR 2002 for Controlled Unclassified Information (CUI)

5. PROCEDURE

SIO, ISO and EPA SO or their official designees for EPA-operated systems; and SM, for systems operated on behalf of the EPA and to the extent made applicable to their management of the system through a contract or other appropriate mechanism, are responsible for implementing the controls in this procedure. EPA is adopting this procedure agency-wide, and expects these officials to develop a plan with timelines for adoption for their system(s). EPA employees, contractors and all other users of EPA information and information systems that support the operations and assets of the EPA should be aware of the content of this procedure and should follow the directions provided by SIO, ISO and EPA SO or their official designees and SM for the systems that they oversee.

The "SA" designator (e.g., SA-2, SA-3) identified for each procedure below corresponds to the NIST- identifier for the System and Services Acquisition control family, as identified in NIST SP 800-53, Revision 5.

NIST defines the applicable SA baseline controls in NIST 800-53B, *Control Baselines for Information Systems and Organizations*. The applicable security baseline for each impact level (Low, Moderate, High or For All Systems) as well as the Privacy Control Baseline are identified below the control name. EPA may deviate from the NIST 800-53B Security or Privacy Control Baselines by adding/removing controls or to applicable baselines and are notated with an asterisk.

SA-2 – Allocation of Resources[1]

For All Systems and Privacy Control Baseline:

1) Determine the high-level information security and privacy requirements for the system or system service in mission and business process planning;
2) Determine, document and allocate the resources required to protect the system or system service as part of the organizational capital planning and investment control process; and
3) Establish a discrete line item for information security and privacy in organizational programming and budgeting documentation.

SA-3 – System Development Life Cycle[2]

For All Systems and Privacy Control Baseline:

1) Acquire, develop, and manage information systems using federal and Agency guidance including but not limited to Federal Acquisition Regulation (FAR), NIST 800-37 and NIST 800-160 v1 and other methodologies such as Agile and Development, Security and Operations (DevSecOps) that incorporates information security and privacy considerations;
2) Define and document information security and privacy roles and responsibilities throughout the system development life cycle;

[1] *This control applies at the organizational level: from top budget planning down through the budgeting and CPIC process.*

[2] *This control applies at the organizational level: through security-related-activities integrated into all EPA IT systems and applications defined in EPA's System Life Cycle Management (SLCM) Policy, section 2. Scope and Applicability.*

3) Identify individuals having information security and privacy roles and responsibilities; and
4) Integrate the organizational information security and privacy risk management process into the system development lifecycle activities.

SA-4 – Acquisition Process
For All Systems and Privacy Control Baseline:

1) Include the following requirements, descriptions, and criteria, explicitly or by reference, using standardized and system-specific, as needed, contract language in the acquisition contract for the system, system component, or system service:
   a) Security and privacy functional requirements;
   b) Strength of mechanism requirements;
   c) Security and privacy assurance requirements;
   d) Controls needed to satisfy the security and privacy requirements;
   e) Security and privacy documentation requirements;
   f) Requirements for protecting security and privacy documentation;
   g) Description of the system development environment and environment in which the system is intended to operate;
   h) Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; and
   i) Acceptance criteria.

SA-4(1) – Acquisition Process | Functional Properties of Controls
For Moderate and High Systems:

1) Require the developer of the system, system component, or system service to provide a description of the functional properties of the controls to be implemented.

SA-4(2) – Acquisition Process | Design and Implementation Information for Controls
For Moderate and High Systems:

1) Require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes: security-relevant external system interfaces, high-level design, low-level design, source code or hardware schematics; at level of sufficient detail to permit independent analysis and testing of the controls.

SA-4(5) – Acquisition Process | System, Component and Service Configurations
For High Systems:

1) Require the developer of the system, system component, or system service to:
   a) Deliver the system, component, or service with secure configurations aligned to EPA approved baseline security configuration guides or other federal and IT guidance (i.e., vendor or manufacturer procedures, best practices, the NIST National Checklist Program (NCP), etc.) implemented, and
   b) Use the configurations as the default for any subsequent system, component, or service reinstallation or upgrade.

SA-4(9) – Acquisition Process | Functions, Ports, Protocols and Services in Use
For Moderate and High Systems:

1) Require the developer of the system, system component, or system service to identify the functions, ports, protocols, and services intended for organizational use.

SA-4(10) – Acquisition Process | Use of Approved PIV Products

For All Systems:

1) Employ only information technology products on the FIPS 201-2 approved products list for Personal Identity Verification (PIV) capability implemented within organizational systems.

SA-5 – Information System Documentation

For All Systems:

1) Obtain or develop administrator documentation for the system, system component, or system service that describes:
    a) Secure configuration, installation, and operation of the information system, component, or service;
    b) Effective use and maintenance of security and privacy functions and mechanisms; and
    c) Known vulnerabilities regarding configuration and use of administrative or privileged functions;
2) Obtain or develop user documentation for the system, system component, or system service that describes:
    a) User-accessible security and privacy functions and how to effectively use those functions and mechanisms;
    b) Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner and protect individual privacy; and
    c) User responsibilities in maintaining the security of the system, component, or service and privacy of individuals;
3) Document attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent and notify the ISO, ISSO, and IMO, as first escalation and OISP as second escalation in response; and
4) Distribute documentation to only those individuals that have been explicitly authorized to review or use the documentation (e.g., system administrators, Information System Security Officers (ISSO), ISO, etc.).

SA-8 – Security and Privacy Engineering Principles

For All Systems:

1) Apply the following systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components: in accordance with NIST guidance e.g., 800-160 Vol. 1 and 2, 800-218 and any other applicable publications.

SA-8(33) – Security and Privacy Engineering Principles | Minimization

For Privacy Control Baseline:

1) Implement the privacy principle of minimization using privacy-enhancing technologies (PETS) that include process documentation such as Privacy Threshold Analysis (PTA), Privacy Impact Assessments (PIA), and System of Record Notices (SORN) reviews (as applicable).

SA-9 – External System Services[3]

For All Systems and Privacy Control Baseline:

1) Require that providers of external system services comply with organizational security and privacy requirements and employ the following controls: security controls in accordance with applicable federal laws, executive orders, directives, policies, regulations, standards, and guidance;
2) Define and document organizational oversight and user roles and responsibilities with regards to external system services; and
3) Employ the following processes, methods, and techniques to monitor control compliance by external providers on an ongoing basis: IT and security contract language and service-level agreements that define the expectations of performance for implemented controls, describe measurable outcomes, and identify remedies and response requirements for identified instances of noncompliance.

SA-9(2) – External System Services | Identification of Functions, Ports, Protocols and Services

For Moderate and High Systems:

1) Require providers of the following external system services to identify the functions, ports, protocols, and other services required for the use of such services: all external information system services supporting EPA e.g. Managed Trusted Internet Protocol Service (MTIPS); Cloud service providers (FedRAMP or otherwise); or managed security service vendors.

SA-10 – Developer Configuration Management

For Moderate and High Systems:

1) Require the developer of the system, system component, or system service to:
   a) Perform configuration management[4] during system, component, or service design, development, implementation, operation, and disposal;
   b) Document, manage and control the integrity of changes to configuration items defined in the Configuration Management Plan referenced in CM-9;
   c) Implement only organization-approved changes to the system, component or service;
   d) Document approved changes to the system, component, or service and potential security and privacy impacts of such changes; and
   e) Track security flaws and flaw resolution within the system, component, or service and report findings to the ISO, ISSO and IMO or Information Resource Management Branch Chief (IRMBC).

[3] *This control applies at the organizational level.*

[4] *Refer to EPA SLCM Procedure, CIO 2121-P-03.1 which establishes the EPA's (Agency) approach and practices in the pre-definition, definition, acquisition/development, implementation, operations and maintenance and termination of EPA information technology (IT) systems and applications. The CMDB tool, a centralized configuration management database, or a series of databases that provide central, logical access to configuration data, containing relevant information such as the configuration items and their attributes, baselines, documentation, changes and relationships, controls EPA's configuration management.*

SA-11 – Developer Testing and Evaluation
For Moderate and High Systems and Privacy Control Baseline:

1) Require the developer of the system, system component, or system service, at all post-design stages of the system development life cycle to:
   a) Develop and implement a plan for ongoing security and privacy control assessments;
   b) Perform unit, integration, system or regression testing/evaluation at least annually or when changes to the system, system component or services may adversely affect previously implemented controls, at an acceptable rigor to demonstrate security controls are operating as intended and that identified risks are minimized prior to any application, or code changes, going into production;
   c) Produce evidence of the execution of the assessment plan and the results of the testing and evaluation;
   d) Implement a verifiable flaw remediation process; and
   e) Correct flaws identified during testing and evaluation.

SA-15 – Development Process, Standards and Tools
For Moderate and High Systems:

1) Require the developer of the system, system component or, system service to follow a documented development process that:
   a) Explicitly addresses security and privacy requirements;
   b) Identifies the standards and tools used in the development process;
   c) Documents the specific tool options and tool configurations used in the development process; and
   d) Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and
2) Review the development process, standards, tools, tool options, and tool configurations annually or when significant changes to security and privacy requirements occur to determine if the process, standards, tools, and tool options and tool configurations selected and employed can satisfy the following security and privacy requirements: delineated in SA-4.

SA-15(3) – Development Process, Standards and Tools | Criticality Analysis
For Moderate and High Systems:

1) Require the developer of the system, system component, or system service to perform a criticality analysis:
   a) At the following decision points in the system development life cycle: at the initial design phase and continuously throughout the development lifecycle when significant changes are made; and
   b) At the following level of rigor: high or low level hardware and software designs, functionality specifications, or source code reviews identify and prioritize security and privacy risks in accordance with the systems' objectives and criticality as specified by the system or application owner or the terms of the contract.

SA-16 – Developer-Provided Training
For High Systems:

1) Require the developer of the system, system component, or system service to provide the following training on the correct use and operation of the implemented security and privacy functions, controls, and/or mechanisms:
   a) Administrator-level training; and

   b) End-user training;

<u>SA-17 – Developer Security and Privacy Architecture and Design</u>
For High Systems:

1) Require the developer of the system, system component, or system service to produce a design specification and security and privacy architecture that:
   a) Is consistent with the organization's security and privacy architecture that is an integral part the organization's enterprise architecture;
   b) Accurately and completely describes the required security and privacy functionality, and the allocation of controls among physical and logical components; and
   c) Expresses how individual security and privacy functions, mechanisms, and services work together to provide required security and privacy capabilities and a unified approach to protection.

<u>SA-21 – Developer Screening</u>
For High Systems:

1) Require that the developer of the information system, system component or service:
   a) Has appropriate access authorizations as determined by assigned roles and responsibilities; and
   b) Satisfies the following additional personnel screening criteria: in accordance with the position risk designation assigned to the developers position as specified by the system or application owner.

<u>SA-22 – Unsupported System Components</u>
For All Systems:

1) Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or
2) Provide the following options for alternative sources for continued support for unsupported components in-house support or as contractually required by vendors and external service providers.

6. ROLES AND RESPONSIBILITIES

The Information Security – Roles and Responsibilities procedure provides roles and responsibilities for personnel who have IT security or related governance responsibility for protecting the information and information systems they operate, manage and support.

7. RELATED INFORMATION

- NIST SP 800-37, Revision 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, December 2018
- NIST SP 800-160 Vol. 1 Revision 1, Engineering Trustworthy Secure Systems, November 2022
- NIST SP 800-160 Vol. 2, Revision 1, Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, December 2021

- NIST SP 800-218, Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities, February 2022
- EPA SLCM Procedure, CIO 2121-P-03.1
- EPA Configuration Management Policy, CIO 2123.2
- EPA CPIC Program Policy, CIO 2120.5
- EPA Information Security Policy
- EPA Roles and Responsibilities Procedures
- EPA CUI Policy
- EPA CUI Procedure

8. DEFINITIONS

- **Code of Federal Regulations**[5] – the codification of the general and permanent rules published in the Federal Register by the departments and agencies of the Federal Government. The C.F.R. contains 50 titles that represent broad areas subject to federal regulation.
- **Configuration Management** – a collection of activities focused on establishing and maintaining the integrity of information technology products and systems, through control of processes for initializing, changing and monitoring the configurations of those products and systems throughout the SDLC.
- **Continuous Monitoring** – maintaining ongoing awareness to support organizational risk decisions.
- **Chain of Trust** – occurs when each component of hardware and software for an information system are validated. The purpose is to ensure that only trusted components are used.
- **External System** – a system or component of a system that is used by but is not a part of an organizational system and for which the organization has no direct control over the implementation of required security and privacy controls or the assessment of control effectiveness.
- **Federal Risk and Authorization Management Program (FedRAMP)** – a government-wide program that provides a standardized approach to security assessment, authorization and continuous monitoring for cloud products and services.
- **Information System** – a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information.
- **Information Technology** – any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information by the executive agency. IT

[5] *Refer to: Chapter 1, Subchapter B, Part B. Subpart C, Information Security Responsibilities for Employees who manage or Use Federal Information Systems, Section 930.301 – Information systems security awareness training program; for employees who manage or use EPA information Systems; and requirements for IS security awareness training program.*

commonly includes computers, ancillary equipment, software, firmware, similar procedures, services and related resources.

- **Plan of Actions & Milestones (POA&M)** – a document that identifies tasks needing accomplishment to remediate identified security weaknesses. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks and scheduled completion dates for the milestones. The purpose of this POA&M is to assist agencies in identifying, assessing, prioritizing and monitoring the progress of corrective efforts for security weaknesses found in programs and systems. (Source: OMB Memo 02-01)
- **Signature** (of an individual) – a mark or sign made by an individual to signify knowledge, approval, acceptance or obligation (can be accomplished manually, sometimes referred to as a “wet signature,” or electronically).
- **System Development Life Cycle** – is the overall process of developing, implementing and retiring information systems through a multistep process from initiation, analysis, design, implementation and maintenance to disposal. There are many different SDLC models and methodologies, but each generally consists of a series of defined steps or phases. For any SDLC model that is used, information security must be integrated into the SDLC to ensure appropriate protection for the information that the system will transmit, process and store.
- **Trustworthiness** – a characteristic or property of an information system that expresses the degree to which the system preserves the confidentiality, integrity and availability of the information processed, stored or transmitted by the system.
- **Trustworthy (System)** – the degree to which an information system (including the information technology components that are used to build the system) can be expected to preserve the confidentiality, integrity and availability of the information being processed, stored or transmitted by the system across the full range of threats.
- **Written** (or in writing) – to officially document the action or decision, either manually or electronically, including a signature.

9. WAIVERS

Waivers or deviations may be requested through the EPA Risk Determination Process based on a substantive business need and the implementation of compensating controls that provide a suitable alternative to the mandated protection.

Only EPA’s Chief Information Officer may authorize Agency-wide waivers or deviations from the standards herein.

10. DIRECTIVE(S) SUPERSEDED

This procedure supersedes Information Directive: CIO-2150.3-P-15.1 Information Security – Interim System and Services Acquisition Procedures, Version 3.1, July 17, 2012.

11. CONTACTS

For information about this directive, please contact the Office of Mission Support (OMS), Office of Information Security and Privacy (OISP) at Infosec@epa.gov.

VAUGHN NOGA Digitally signed by VAUGHN NOGA
Date: 2023.12.19 13:39:44 -05'00'

Vaughn Noga, Chief Information Officer and Deputy Assistant Administrator for Information Technology and Information Management

APPENDIX A: ACRONYMS & ABBREVIATIONS

C.F.R.	Code of Federal Regulations
CIO	Chief Information Officer
CM	Configuration Management
CPIC	Capital Planning and Investment Control
DevSecOps	Development, Security and Operations
EPA	Environmental Protection Agency
FAR	Federal Acquisition Regulation
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization
IRMBC	Information Resource Management Branch Chief
ISO	Information Security Officers
ISSO	Information System Security Officers
IT	Information Technology
MTIPS	Managed Trusted Internet Protocol Service
NCP	National Checklist Program
NIST	National Institute of Standards and Technology
OISP	Office of Information Security and Privacy
OMS	Office of Mission Support
PETS	Privacy-Enhancing Technologies
PII	Personally Identifiable Information
POA&M	Plan of Actions & Milestones
SA	System and Services Acquisition
SDLC	System Development Life Cycle
SIO	Senior Information Officials
SLCM	System Life Cycle Management
SM	Service Managers
SO	System Owners
SP	Special Publication
SSDF	Secure Software Development Framework
SSN	Social Security Number
U.S.C.	United States Code