EPA **IT/IM DIRECTIVE**
PROCEDURE

Information Security – System and Communications Protection (SC) Procedure

Directive No: CIO 2150.3-P-16.2

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

Information Security – System and Communications Protection (SC) 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 Communications Protection (SC) 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

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 "SC" designator (e.g., SC-2, SC-3) identified for each procedure below corresponds to the NIST- identifier for the System Communications Protection control family, as identified in NIST SP 800-53, Revision 5.

NIST defines the applicable SC security and privacy baseline controls in NIST SP 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.

SC-2 – Separation of System and User Functionality

For Moderate and High Systems:

1) Separate user functionality, including user interface services, from system management functionality.

SC-3 – Security Function Isolation

For High Systems:

1) Isolate security functions from non-security functions.

SC-4 – Information in Shared System Resources

For Moderate and High Systems:

1) Prevent unauthorized and unintended information transfer via shared system resources.

SC-5 – Denial-of-Service Protection

For All Systems:

1) Protect against or limit the effects of the following (or similar) types of denial-of-service events: volume-based; protocol flooding/attacks; and application layer attacks; and
2) Employ the following controls to achieve the denial-of-service objective: EPA approved safeguards to include but not limited to: security monitoring, host-based protections, boundary protection, network capacity and bandwidth management, and service redundancy.

SC-7 – Boundary Protection

For All Systems:

1) Monitor and control communications at the external managed interfaces to the system

and at key internal managed interfaces within the system;
2) Implement subnetworks for publicly accessible system components that are logically separated from internal organizational networks; and
3) Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.

SC-7(3) – Boundary Protection | Access Points

For Moderate and High Systems:

1) Limit the number of external network connections to the system.

SC-7(4) – Boundary Protection | External Telecommunications Services

For Moderate and High Systems:

1) Implement a managed interface for each external telecommunication service;
2) Establish a traffic flow policy for each managed interface;
3) Protect the confidentiality and integrity of the information being transmitted across each interface;
4) Document each exception to the traffic flow policy with a supporting mission or business need and the duration of that need;
5) Review exceptions to the traffic flow policy every six (6) months and remove exceptions that are no longer supported by an explicit mission or business need;
6) Prevent unauthorized exchange of control plane traffic with external networks;
7) Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks; and
8) Filter unauthorized control plane traffic from external networks.

SC-7(5) – Boundary Protection | Deny by Default — Allow by Exception

For Moderate and High Systems:

1) Deny network communications traffic by default and allow network communications traffic by exception at all managed interfaces for applicable EPA information systems.

SC-7(7) – Boundary Protection | Split Tunneling for Remote Devices

For Moderate and High Systems:

1) Prevent split tunneling for remote devices connecting to EPA systems unless the split tunnel is securely provisioned using Office of Mission Support (OMS) Office of Information Technology and Operations (OITO) configuration standards.

SC-7(8) – Boundary Protection | Route Traffic to Authenticated Proxy Servers

For Moderate and High Systems:

1) Route only authorized internal communications traffic to explicitly defined (via IP address or other unique identifier) external networks through authenticated proxy servers at managed interfaces.

SC-7(18) – Boundary Protection | Fail Secure

For High Systems:

1) Prevent systems from entering unsecure states in the event of an operational failure of a boundary protection device.

SC-7(21) – Boundary Protection | Isolation of System Components
For High Systems:
1) Employ boundary protection mechanisms to isolate systems components supporting regional/program office defined missions and/or business functions.

SC-7(24) – Boundary Protection | Personally Identifiable Information
For Privacy Control Baseline:
1) For systems that process personally identifiable information:
   a) Apply the following processing rules to data elements of personally identifiable information: as defined in the Protecting Personally Identifiable (PII) Procedure;
   b) Monitor for permitted processing at the external interfaces to the system and at key internal boundaries within the system;
   c) Document each processing exception; and
   d) Review and remove exceptions that are no longer supported.

SC-8 – Transmission Confidentiality and Integrity
For All Systems*:
1) Protect the integrity and confidentiality of transmitted information.

SC-8(1) – Transmission Confidentiality and Integrity | Cryptographic Protection
For All Systems*:
1) Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of information during transmission.

SC-10 – Network Disconnect
For Moderate and High Systems:
1) Terminate the network connection associated with a communications session at the end of the session or after ninety (90) minutes of inactivity.

SC-12 – Cryptographic Key Establishment and Management
For All Systems:
1) Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: outlined in NIST SP 800-57 and EPA defined standards.

SC-12(1) – Cryptographic Key Establishment and Management | Availability
For High Systems:
1) Maintain availability of information in the event of the loss of cryptographic keys by users.

SC-13 – Cryptographic Protection
For All Systems:
1) Determine the cryptographic uses to protect the identity, network, devices, data and applications; and
2) Implement the following types of cryptography required for each specified cryptographic use: NIST FIPS-compliant or NSA-approved cryptographic standards[1].

[1] *The current federal standard for employing cryptography in information systems is FIPS 140-3; however, FIPS 140-2 may be used until 5 years after validation or until September 21, 2026*

SC-15 – Collaborative Computing Devices

For All Systems:

1) Prohibit remote activation of collaborative computing devices and applications with the following exceptions: those explicitly authorized for use by the EPA; and
2) Provide an explicit indication of use to users physically present at the devices.

SC-17 – Public Key Infrastructure Certificates

For Moderate and High Systems:

1) Issue public key certificates under the EPA Enterprise Public Key Infrastructure (PKI) Certificate services or obtain public key certificates from an approved service provider; and
2) Include only approved trust anchors in trust stores or certificate stores managed by the organization.

SC-18 – Mobile Code

For Moderate and High Systems:

1) Define acceptable and unacceptable mobile code and mobile code technologies; and
2) Authorize, monitor and control the use of mobile code within the information system.

SC-20 – Secure Name/Address Resolution Service (Authoritative Source)

For All Systems:

1) Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and
2) Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

SC-21 – Secure Name/Address Resolution Service (Recursive or Caching Resolver)

For All Systems:

1) Request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

SC-22 – Architecture and Provisioning for Name/Address Resolution Service

For All Systems:

1) Ensure the systems that collectively provide name/address resolution services for an organization are fault-tolerant and implement internal and external role separation.

SC-23 – Session Authenticity

For Moderate and High Systems:

1) Protect the authenticity of communications sessions.

SC-24 – Fail in Known State

For High Systems:

1) Fail to a known secure system state for the following failures on the indicated components while preserving the confidentiality, integrity, and availability of critical information in failure: all system failures for components that directly support essential mission functions.

SC-28 – Protection of Information at Rest

For All Systems*:

1) Protect the confidentiality and integrity of the following information at rest: all user, application and system information included in both online and offline storage.

SC-28(1) – Protection of Information at Rest | Cryptographic Protection

For All Systems*:

1) Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on all Government Furnished Equipment (GFE) or non-GFE contractor managed system components, databases, storage devices and media including Universal Serial Bus (USB), internal and external hard drives, and shared storage space: all user, application and system information.

SC-28(2) – Protection of Information at Rest | Off-Line Storage

For All Systems*:

1) Remove the following information from online storage and store offline in a secure location: as explicitly defined by the SO and ISO in lieu of protecting such information online.

SC-28(3) – Protection of Information at Rest | Cryptographic Keys

For All Systems*:

1) Provide protected storage for cryptographic keys using a Trusted Platform Module (TPM) or similar key store that meets or exceeds federal FIPS 140-2/3 requirements.

SC-39 – Process Isolation

For All Systems:

Maintain a separate execution domain for each executing system process.

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 Cryptographic Module Validation Program
- NIST SP 800-57 Part 2, Rev 1, Recommendation for Key Management: Part 2 – Best Practices for Key Management Organizations
- EPA Information Security Policy
- EPA Roles and Responsibilities Procedures

8. DEFINITIONS

- **Active Content** – electronic documents and other objects that can carry out or trigger actions automatically on a computer platform without the intervention of a user.

- **Boundary Protection** – monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications using boundary protection devices.
- **Boundary Protection Device** – a device (e.g., gateway, router, firewall, guard or encrypted tunnel) that facilitates the adjudication of different system security policies for connected systems or provides boundary protection. The boundary may be the authorization boundary fora system, the organizational network boundary or a logical boundary defined by the organization.
- **Collaborative Computing** – an interactive multimedia conferencing application that enables multiple parties to collaborate on text and graphic documents. Through special software, each party to the call can contribute to such documents, working together with the other parties. During such a collaborative session, the original text document is saved, while each party contributes changes that are identifiable by contributor. When the parties agree to the collaborative edits and enhancements, the entire text file is refreshed and saved. Similarly, a design or a concept can be developed graphically and modified on a collaborative basis through white boarding, much as the parties would do on a physical whiteboard in a face-to-face meeting. Typically, each party to the conference has access to a special whiteboard pad and stylus, which is used to draw. Each party can modify the initial drawing, with everyone’s contribution identified by separate color. Once the group has agreed on the final graphic rendition, the graphic is saved and all screens are refreshed (Webster’s New World Telecom Dictionary).
- **Confidentiality** – the preservation of authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- **External Networks** – networks outside the control of the organization.
- **Information at Rest** – the state of information when it is located on a secondary storage device (e.g., disk drive, tape drive) within an organizational information system.
- **Information System Management Functionality** – functions necessary to administer databases, network components, workstations or servers and typically require privileged users’ access.
- **Integrity** – to guard against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.
- **Mobile Agent** – a type of mobile code that is autonomous and intelligent and can migrate from machine to machine throughout a heterogeneous network, deciding when and where to migrate, and maintain its state. Mobile agents initiate their own execution and migration from one platform to another without any user interaction. A supporting mobile agent platform typically resides on a machine to receive migrating mobile agents at runtime. Mobile agents may be implemented as scripts, intermediate languages (e.g., Java) or binary executables (e.g., C++).
- **Mobile Agent Technologies** – software technologies that provide the mechanisms for the production and use of mobile agents (e.g., Tool command language [Tcl], Aglets).
- **Mobile Code** – software programs or parts of programs obtained from remote information systems, transmitted across a network and executed on a local information system without explicit installation or execution by the recipient.
- **Mobile Code Technologies** – software technologies that provide the mechanism for the production and use of mobile code (e.g., Java, JavaScript, ActiveX,

VBScript, Java Virtual Machine, Java compiler, .NET Common Language Runtime, Windows Scripting Host, HTML Application Host).

- **Object Reuse** – control of information in shared resources.
- **Protective Distribution System** – wire line or fiber optic system that includes adequate safeguards and/or countermeasures (e.g., acoustic, electric, electromagnetic and physical) to permit its use for the transmission of unencrypted information.
- **Permitted Mobile Code** – types of mobile code that are allowed to be used in accordance with this Procedure when the associated usage requirements are implemented. Permitted mobile code includes signed Category 1A mobile code, unsigned Category 2 mobile code that executes in a constrained execution environment, Category 2 mobile code obtained from a trusted source over an assured channel, Category 3 mobile code and mobile code that downloads via email that does not execute automatically when the user opens the email body or attachment.
- **Prohibited Mobile Code** – types of mobile code that are prohibited from being used in EPA information systems in accordance with this procedure. Prohibited mobile code includes all unapproved Category 1X mobile code, unapproved and unsigned Category 1A mobile code, Category 2 mobile code that violates this Procedure’s usage requirements, all emerging technologies mobile code and all mobile code that downloads via an email body or email attachment that executes automatically when the user opens the email body or attachment.
- **Sensitive Information** – information, the loss, misuse, or unauthorized access to or modification of, that could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.
- **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).
- **Written (or in writing)** – to officially document the action or decision, either manually or electronically, and includes 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-16.1 Information Security – Interim System and Communications Protection Procedures, Version 3.1, July 16, 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: 2023.11.21 14:11:14 -05'00'

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

APPENDIX A: ACRONYMS & ABBREVIATIONS

CIO	Chief Information Officer
CISO	Chief Information Security Officer
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
EPA	Environmental Protection Agency
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
HSPD	Homeland Security Program Directive
HTML	Hypertext Markup Language
IO	Information Owner
ISO	Information Security Officer
ISSO	Information System Security Officer
NIST	National Institute of Standards and Technology
OLEM	Office of Land and Emergency Management
OMB	Office of Management and Budget
OMS	Office of Mission Support
OITO	Office of Information Technology Operations
OISP	Office of Information Security and Privacy
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
SA	System Administrator
SIO	Senior Information Official
SM	Service Manager
SO	System Owner
SP	Special Publication
U.S.C.	United States Code
VoIP	Voice over Internet Protocol