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

Information Security – Supply Chain Risk Management (SR) 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 Supply Chain Risk Management Family (SR), 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
- Executive Order 14028, Improving the Nation's Cybersecurity, May 12, 2021
- 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

- NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
- NIST SP 800-161, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations

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 though 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 "SR" designator (e.g., SR-2, SR-3) identified for each procedure below corresponds to the NIST- identifier for the Supply Chain Risk Management control family, as identified in NIST SP 800-53, Revision *5.*

NIST defines the applicable SR 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.

SR-2 – Supply Chain Risk Management Plan

For All Systems:

1) Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the following systems, system components or system services: all systems, system components, and services in the FISMA inventory e.g. hardware (HW), firmware, operating systems, software (SW), and Information, Communications and Technology (ICT) services;
2) Review and update the supply chain risk management (SCRM) plan annually or as required, to address threat, organizational or environmental changes; and
3) Protect the supply chain risk management plan from unauthorized disclosure and modification.

SR-2(1) – Supply Chain Risk Management Plan | Establish SCRM Team

For All Systems:

1) Establish a supply chain risk management team consisting of SCRM Senior Agency Official (SAO), ICT SCRM Program Manager, and others as designated by the SCRM SAO to lead and support the following SCRM activities:
   a) Frame ICT SCRM risks in accordance with the Agency risk management strategy;
   b) Assess ICT SCRM risks based upon current version of NIST SP 800-30, NIST SP 800-53, and other assessment methodologies when identified and authorized for use by the Agency;
   c) Respond to ICT SCRM risks by following the EPA Plan of Actions and Milestones (POA&M) process; and
   d) Monitor ICT SCRM risks in accordance with the current version of NIST SP 800-137 and the re-assessment preconditions defined by the Agency.

SR-3 – Supply Chain Controls and Processes

For All Systems:

1) Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of all systems and their components in coordination with EPA enterprise and mission stakeholders defined within the SCRM Strategic Plan;
2) Employ the following controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain related events: Agency defined controls detailed within the EPA policy and procedures; and
3) Document the selected and implemented supply chain processes and controls in system security and privacy plans and system-specific supply chain risk management plans.

SR-5 – Acquisition Strategies, Tools, and Methods

For All Systems:

1) Employ the following acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks: ICT vendor and supplier attestation of conformance to current version of NIST SP 800-161; ICT vendor and supplier self-attestation of compliance with Section 889 of the FY 2019 National Defense Authorization Act (NDAA) Part B; ICT vendor and supplier support in complying with Executive Order (EO) 14028; and ICT vendor and supplier joint training artifacts with EPA ICT SCRM stakeholders.

SR-6 – Supplier Assessments and Reviews

For Moderate and High Systems:

1) Assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide each fiscal year (annually) or upon the identification of evolving threats, issuance of new or significantly changed existing Federal laws, executive orders, directives, regulations, and Agency policies, identification of emerging technology and information technology

service delivery models and determination that adjustments are deemed necessary to improve its effectiveness.

SR-8 – Notification Agreements

For All Systems:

1) Establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the notification of supply chain compromises; results of assessments or audits; and changes in entities involving foreign ownership or business relations.

SR-9 – Tamper Resistance and Detection

For High Systems:

1) Implement a tamper protection program for the system, system component, or system service.

SR-9(1) – Tamper Resistance and Detection | Multiple Stages of System Development Life Cycle

For High Systems:

1) Employ anti-tamper technologies, tools, and techniques throughout the system development life cycle.

SR-10 – Inspection of Systems or Components

For All Systems:

1) Inspect the following systems or system components in accordance with Agency counterfeit detection procedures to detect tampering of software and hardware documented in the system inventory.

SR-11 – Component Authenticity

For All Systems:

1) Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system; and
2) Report counterfeit system components to Computer Security Incident Response Capability (CSIRC) via the Enterprise Information Technology Service Desk (EISD), ISO, warehouse personnel and COR for further action.

SR-11(1) – Component Authenticity | Anti-Counterfeit Training

For All Systems:

1) Train EPA personnel involved in supply chain activities (e.g., ISSO, system administrator, warehouse personnel, etc.) to detect counterfeit system components (including hardware, software, and firmware).

SR-11(2) – Component Authenticity | Configuration Control for Component Service and Repair

For All Systems:

1) Maintain configuration control over the following system components awaiting service or repair and serviced or repaired components awaiting return to service: all components being serviced or repaired.

SR-12 – Component Disposal

For All Systems:

1) Dispose of data, documentation (paper-based and digital files), tools, or system components throughout the system development lifecycle using the following techniques and methods: outlined in the Information Security - Media Protection Procedure, the current version of NIST SP 800-88 and Agency counterfeit detection procedures.

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

- EPA Information Security Policy
- EPA Roles and Responsibilities Procedures
- EPA SCRM Strategic Plan
- NIST SP 800-30, Guide for Conducting Risk Assessments
- NIST SP 800-88, Guidelines for Media Sanitization
- FY 2019 National Defense Authorization Act (NDAA)

8. DEFINITIONS

- **Acquirer** – Stakeholder that acquires or procures a product or service.
- **Acquisition** – Includes all stages of the process of acquiring product or service, beginning with the process for determining the need for the product or service and ending with contract completion and closeout.
- **Critical component** – A system element that, if compromised, damaged, or failed, could cause a mission or business failure.
- **Defense-in-Breadth** – A planned, systematic set of multidisciplinary activities that seek to identify, manage, and reduce risk of exploitable vulnerabilities at every stage of the system, network, or subcomponent life cycle (system, network, or product design and development; manufacturing; packaging; assembly; system integration; distribution; operations; maintenance; and retirement).

- **Defense-in-Depth** – Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and dimensions of the organization.
- **Defensive Design** – Design techniques which explicitly protect supply chain elements from future attacks or adverse events. Defensive design addresses the technical, behavioral, and organizational activities. It is intended to create options that preserve the integrity of the mission and system function and its performance to the end user or consumer of the supply chain element.
- **ICT Supply Chain** – Linked set of resources and processes between acquirers, integrators, and suppliers that begins with the design of ICT products and services and extends through development, sourcing, manufacturing, handling, and delivery of ICT products and services to the acquirer.

  Note: An ICT supply chain can include vendors, manufacturing facilities, logistics providers, distribution centers, distributors, wholesalers, and other organizations involved in the design and development, manufacturing, processing, handling, and delivery of the products, or service providers involved in the operation, management, and delivery of the services.
- **ICT Supply Chain Risk** – Risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.
- **ICT Supply Chain Risk Management** – The process of identifying, assessing, and mitigating the risks associated with the global and distributed nature of ICT product and service supply chains.
- **Information and Communications Technologies (ICT)** – Encompasses the capture, storage, retrieval, processing, display, representation, presentation, organization, management, security, transfer, and interchange of data and information.
- **Risk Mitigation** – Prioritizing, evaluating, and implementing the appropriate risk reducing controls/countermeasures recommended from the risk management process.
- **Supplier** – Organization or individual that enters into an agreement with the acquirer or integrator for the supply of a product or service. This includes all suppliers in the supply chain.
- **Supply Chain Assurance** – Confidence that the supply chain will produce and deliver elements, processes, and information that function as expected.
- **System Development Life Cycle (SDLC)** – The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation.
- **System Owner (SO)** – Person or organization having responsibility for the development, procurement, integration, modification, operation and maintenance, and/or final disposition of an information system.

- **Vulnerability** – Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

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

Not applicable.

11. CONTACTS

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

VAUGHN NOGA Digitally signed by VAUGHN NOGA
Date: 2023.11.21 14:10:25 -05'00'

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

APPENDIX A: ACRONYMS AND ABBREVIATIONS

AO	Authorizing Official
CIO	Chief Information Officer
CISO	Deputy Chief Information Security Officer
EPA	Environmental Protection Agency
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
ICT	Information and Communication Technology
ISO	Information Security Officer
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OMS	Office of Mission Support
OISP	Office of Information Security and Privacy
OITO	Office of Information Technology Operations
OPSEC	Operation Security
SR	Supply Chain Risk Management
SDLC	System Development Lifecycle
SO	System Owner
SP	Special Publication
U.S.C.	United States Code