Information Technology (IT) System Supply Chain Risk Management (SR) Standard

January 31, 2022

U.S. Department of Education (ED)

Office of the Chief Information Officer (OCIO)

Information Assurance Services (IAS)

Questions about the policies outlined in this document should be directed to Information Assurance Services (IAS) at **OCIO_IAS@ed.gov**

APPROVAL

Steven Hernandez

Digitally signed by Steven Hernandez
Date: 2022.02.01 16:09:47 -05'00'

Steven Hernandez
Director, IAS/Chief Information Security Officer (CISO)

Revision History

The table below identifies all changes that have been incorporated into this document.

Version	Draft Date	Summary of Changes
1.0	1/21/2022	Initial draft of new standard which combines NIST SP 800-53, Revision 5 controls, including ED specific control parameter values, with existing policy standards.
1.1	1/31/2022	Update to incorporate feedback from IAS; address new security measures required by Executive Order (EO) 14028, including Office of Management and Budget (OMB) regulations and memoranda and updated NIST guidance issued to comply with the EO.

Table of Contents

1 INTRODUCTION

1.1 Purpose

The Federal Information Security Modernization Act (FISMA)[1] and implementing regulation Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*[2], requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, and services that are either fully or partially provided, including agency-hosted, outsourced, and cloud-based solutions. Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*[3], mandates the use of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Information Systems and Organizations*[4], as baseline information system controls.

This governance document establishes Department information technology (IT) system supply chain risk management controls standards necessary to improve the efficiency of operation or security of Department information systems and comply with Federal laws, regulations, Executive Orders, Emergency Orders, Binding Operational Directives, and Department Administrative Communications System (ACS) directives and policies. In doing so, these standards supersede any prior governance documentation establishing such standards.

1.2 Scope

These standards apply to all information and information systems that support the operations and assets of the Department, including those provided or managed by another agency, contractor, or other source, as well as services that are either fully or partially provided, including Department-hosted, outsourced, and cloud-based solutions. Principal Offices, employees, contractors, external service providers and system users are required to comply with these supply chain risk management control standards.

2 STANDARDS

The Department standards for IT system supply chain risk management are organized to follow the order in which controls are presented in the current version of NIST SP 800-53. To define a control baseline for Department information systems, a FIPS 199 categorization level (e.g., Low (L), Moderate (M) and High (H)) is assigned to each requirement. This designator indicates a

[1] Public Law 113-283-Dec. 18, 2014, https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf
[2] Office of Management and Budget (OMB) Circular A-130, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf
[3] FIPS 200, https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.200.pdf
[4] NIST SP 800-53, https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

requirement applies to information systems categorized at that FIPS 199 impact-level. Designators are also used to indicate when NIST SP 800-53 Privacy (P) baseline controls are required. To manage risk to within the Department's risk tolerance and appetite, control overlays are provided when the Department requires implementation of control(s) that are not required by the FIPS 199 impact-level or privacy baseline. In addition to the controls required by this standard, High Value Assets (HVAs) must implement and comply with the current version of the HVA Control Overlay issued and maintained by the Department of Homeland Security (DHS), Cybersecurity & Infrastructure Security Agency (CISA).

This standard directly supports the Department's integration of the NIST Cyber Security Framework (CSF) in focusing on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the Department's risk management processes. Refer to Appendix A for a summary of controls by baseline and corresponding NIST CSF categories and subcategories.

2.1 SR-1 Supply Chain Risk Management System Policy and Procedures (L, M, H)

The Department shall develop, document, and disseminate to all ED employees, contractors, and users authorized to access to ED information systems, or systems operated or maintained on behalf of ED, or ED information as defined in OCIO: 3-112/ACSD-OCIO-004, *Cybersecurity Policy* a Department-level IT supply chain risk management policy (e.g., this document) that:

(a) addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

(c) authorizes the Department Chief Information Security Officer (CISO) and Department Chief Information Officer (CIO) to issue subordinate standards, procedures, and memos, with the same authority and enforcement as OCIO: 3-112/ACSD-OCIO-004, Cybersecurity Policy.

The Department CISO in conjunction with the Senior Agency Official for Privacy (SAOP) are designated to manage the development, documentation, and dissemination of the Department-level IT supply chain risk management policy.

This policy shall be reviewed and updated annually (i.e., each fiscal year) and following the identification of evolving threats, issuance of new or significantly changed existing Federal laws, executive orders, directives, regulations, and ED policies, identification of emerging technology and information technology service delivery models and determination that adjustments are deemed necessary to improve its effectiveness based upon feedback from Principal Office personnel.

The Office of the Chief Information Officer (OCIO), Information Assurance Services (IAS) manage the development, documentation, and dissemination of the Department-level supply

chain risk management standard operating procedures in support of this policy standard. IAS Branch Chiefs shall review these procedures annually (i.e., each fiscal year) and following the identification of evolving threats, issuance of new or significantly changed existing Federal laws, executive orders, directives, regulations, and ED policies, identification of emerging technology and information technology service delivery models and determination that adjustments are deemed necessary to improve its effectiveness based upon feedback from Principal Office personnel.

Principal Office Information System Owners (ISO) and Information System Security Officers (ISSOs) are required to manage the development, documentation, and dissemination of system specific procedures to facilitate the implementation of this policy standard and associated IT supply chain risk management controls. The ISO and ISSO shall review IT supply chain risk management procedures annually (i.e., each fiscal year) and following the identification of evolving threats, issuance of new or significantly changed existing Federal laws, executive orders, directives, regulations, and ED policies, identification of emerging technology and information technology service delivery models and determination that adjustments are deemed necessary to improve its effectiveness based upon feedback from Principal Office personnel.

2.2 SR-2 Supply Chain Risk Management Plan (L, M, H)

a. 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 within the Department's FISMA inventory;

b. Review and update the supply chain risk management plan annually (i.e., each fiscal year) or as required, to address threat, organizational or environmental changes; and

c. Protect the supply chain risk management plan from unauthorized disclosure and modification.

2.2.1 SR-2(1) Supply Chain Risk Management Plan | Establish SCRM Team (L, M, H)

Establish a supply chain risk management (SCRM) team consisting of SCRM Senior Agency Official, Information and Communications Technology (ICT) SCRM Program Manager, ICT SCRM Team, CISO, CIO, ISSO, ISO, Contracting Officer (CO) and Contracting Officer Representative (COR) to lead and support the following SCRM activities:

a. Frame ICT SCRM risks based upon ED risk tolerance levels and multi-tiered risk management roles and responsibilities at the organizational, mission, and information system level;

b. Assess ICT SCRM risks based upon current version of NIST SP 800-30, Committee on National Security Systems Instruction (CNSSI) 4009, NIST SP 800-53, and other assessment methodologies when identified and authorized for use by the Department;

c. Respond to ICT SCRM risks by following the ED Plan of Actions and Milestones (POA&M) process;

d. Monitor ICT SCRM risks in accordance with the current version of NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* guidance, Department risk tolerance levels, and the re-assessment preconditions defined by the Department.

2.3 SR-3 Supply Chain Controls and Processes (L, M, H)

a. Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of Department systems and their components in coordination with Department enterprise and mission stakeholders defined within the ICT SCRM Roadmap;

b. 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: Department organizationally defined controls detailed in the ED ICT SCRM Strategy; and

c. Document the selected and implemented supply chain processes and controls in the system security plan.

2.3.1 SR-3(3) Supply Chain Controls and Processes | Sub-tier Flow Down (Control Overlay)

Not applicable to Privacy Baseline or Security Control Baseline for Low, Moderate, or High systems; supply chain overlay applies.

Control Overlay SR-3(3) ED-01 (L, M, H): Require Tier 1 (prime) contractors to include processes within risk management plans and SLAs to ensure sub-tier contractors implement SR-3(b), SR-5, and SR-8 controls.

2.4 SR-4 Provenance (Control Overlay)

Not applicable to Privacy Baseline or Security Control Baseline for Low, Moderate, or High systems; supply chain overlay applies.

Control Overlay SR-4 ED-01 (H): Obtain software bill of materials (SBOM) documentation and report receipt of documentation to the ICT SCRM Team.

2.4.1 SR-4(1) Provenance | Identity (Control Overlay)

Control not applicable to Privacy Baseline or Security Control Baseline for Low, Moderate, or High systems; supply chain overlay applies.

Control Overlay SR-4(1) ED-01 (H): Ensure Tier 1 (prime) suppliers maintain visibility into supply chain activities by requiring supplier self-attestation to ED and conducting periodic supply chain risk assessments to validate control implementation.

2.4.2 SR-4(2) Provenance | Track and Trace (Control Overlay)

Control is not applicable to Privacy Baseline or Security Control Baseline for Low, Moderate, or High systems; supply chain overlay applies.

Control Overlay SR-4(2) ED-01 (H): Label all hardware using serial numbers or radio frequency identification tags. Shipping delays or lost inventory must be reported to the ICT SCRM Team.

Control Overlay SR-4(2) ED-02 (H): Report shipping delays or lost inventory to the ICT SCRM Team.

2.5 SR-5 Acquisition Strategies, Tools, and Methods (L, M, H and Control Overlay)

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, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*; 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 reporting of supply chain cyber incidents to EDSOC; ICT vendor and supplier support in complying with Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*; and ICT vendor and supplier joint training with ED ICT SCRM stakeholders

2.5.1 SR-5(2) Acquisition Strategies, Tools, and Methods | Assessments Prior to Selection, Acceptance, Modification, or Update (Control Overlay)

Control is not applicable to Privacy Baseline or Security Control Baseline for Low, Moderate, or High systems; supply chain overlay applies.

Control Overlay SR-5(2) ED-01 (L, M, H): Evaluate the SBOM prior to the use of software.

Control Overlay SR-5(2) ED-02 (L, M, H): Conduct physical inspection of hardware deliveries prior to the use of hardware and submit physical inspection results to the ICT SCRM Team.

2.6 SR-6 Supplier Assessments and Reviews (M, H)

Assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide annually (i.e., each fiscal year) or upon the identification of evolving threats, issuance of new or significantly changed existing Federal laws, executive orders, directives, regulations, and Department policies, identification of emerging technology and information technology service delivery models and determination that adjustments are deemed necessary to improve its effectiveness based upon feedback from Principal Office personnel.

2.6.1 SR-6(1) Supplier Assessments and Reviews | Testing and Analysis (Control Overlay)

Control not applicable to Privacy Baseline or Security Control Baseline for Low, Moderate, or High systems; supply chain overlay applies.

Control Overlay SR-6(1) ED-01 (M, H): Conduct supplier risk assessments in accordance with the ICT supply chain risk assessment schedule.

2.7 SR-8 Notification Agreements (L, M, H)

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; for all instances of IT system compromises impacting Department systems.

2.8 SR-9 Tamper Resistance and Detection (H)

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

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

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

2.9 SR-10 Inspection of Systems or Components (L, M, H)

Inspect the following systems or system components: software and hardware documented in the system inventory, annually (i.e., each fiscal year), or upon indications of need for inspection by the ICT SCRM Team. Asset managers will inspect deliverables prior to use and consult with the ICT SCRM Team as needed to detect tampering; the inspection of systems or components, inspections of packaging modifications, review of delivery invoices, and other physical properties for indications of a potential compromise will address physical and logical tampering. Software hashes will be inspected and the SBOM reviewed prior to use.

2.10 SR-11 Component Authenticity (L, M, H)

a. Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system; and

b. Report counterfeit system components to the EDSOC, ICT SCRM Team, and ISSO for further action.

2.10.1 SR-11(1) Component Authenticity | Anti-counterfeit Training (L, M, H)

Train ICT SCRM Team, hardware and software asset managers and others responsible for hardware and software inventories to detect counterfeit system components (including hardware, software, and firmware).

2.10.2 SR-11(2) Component Authenticity | Configuration Control for Component Service and Repair (L, M, H)

Maintain configuration control over the following system components awaiting service or repair and serviced or repaired components awaiting return to service: All components.

2.11 SR-12 Component Disposal (L, M, H)

Dispose of data, documentation (paper-based and digital files), tools, and system components throughout the system development lifecycle using the following techniques and methods: Enterprise Review Board Checklist, System Retirement Plan, Information Technology (IT) System Media Protection (MP) Standard and the current version of NIST SP 800-88*, Guidelines for Media Sanitization*.

3 RISK ACCEPTANCE/POLICY EXCEPTIONS

Deviations from the Department policies, Instructions, Standards, Procedures or Memos must be approved and documented through the Department's Risk Acceptance process. Deviations that introduce additional risks to the enterprise must be submitted through the Department Risk Acceptance Form (RAF) and must be approved by the ED CISO (as delegated). Requests must justify the reason for the deviation(s)/exception(s) as well as the compensating security controls implemented to secure the device or information, if applicable. Policy deviations that do not introduce additional risks do not need to be submitted through the Department RAF but will need to be approved by the Department CISO (as delegated).

4 ACRONYMS

ACS	Administrative Communications System
CIO	Chief Information Officer
CISA	Cybersecurity & Infrastructure Security Agency
CISO	Chief Information Security Officer
CNSSI	Committee on National Security Systems Instruction
CO	Contract Officer
COR	Contracting Officer's Representative
DHS	Department of Homeland Security
ED	Department of Education
EDSOC	ED Security Operations Center
EPMR	Enterprise Program Management Review
EO	Executive Order
FIPS	Federal Information Processing Standard
HVA	High Value Asset
IAS	Information Assurance Services
ICT	Information and Communications Technology
ISO	Information System Owner
ISSO	Information Systems Security Officer
IT	Information Technology
NIST	National Institute of Standards and Technology
NDAA	National Defense Authorization Act
OMB	Office of Management and Budget
PO	Principal Office
POA&M	Plan of Action and Milestones
RAF	Risk Acceptance Form
SAOP	Senior Agency Official for Privacy
SBOM	Software Bill of Materials
SCRM	Supply Chain Risk Management

SLA	Service Level Agreement
SP	Special Publication

5 APPENDIX A - BASELINE CONTROL PARAMETER SUMMARY

The applicability for each baseline control parameter is shown below. NIST SP 800-53 controls that are not applicable to any control baseline are shaded in gray.

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
SR-1	Policy and Procedures		x	x	x	ID.BE, ID.SC, DE.DP, ID.GV, GV.PO-P, GV.MT-P, ID.BE-P, ID.DE-P	ID.BE-1, ID.SC-1, DE.DP-2, ID.GV-1, ID.GV-3, GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.MT-P2, GV.MT-P6, ID.BE-P1, ID.DE-P1
SR-2	Supply Chain Risk Management Plan		x	x	x	ID.BE, ID.SC, ID.DE-P	ID.BE-4, ID.SC-1, ID.SC-2, ID.SC-3, ID.DE-P1, ID.DE-P2, ID.DE-P3
SR-2(1)	Supply Chain Risk Management Plan | Establish SCRM Team		x	x	x	ID.BE, ID.SC, ID.DE-P	ID.BE-4, ID.SC-1, ID.SC-2, ID.SC-3, ID.DE-P1, ID.DE-P2, ID.DE-P3
SR-3	Supply Chain Controls and Processes		x	x	x	ID.BE, ID.SC, ID.BE-P, ID.DE-P	ID.BE-1, ID.SC-1, ID.SC-2, ID.SC-3, ID.BE-P1, ID.DE-P1, ID.DE-P2, ID.DE-P3
SR-3(1)	Supply Chain Controls and Processes | Diverse Supply Base					ID.BE, ID.SC, ID.BE-P, ID.DE-P	ID.BE-1, ID.SC-1, ID.SC-2, ID.SC-3, ID.BE-P1, ID.DE-P1, ID.DE-P2, ID.DE-P3
SR-3(2)	Supply Chain Controls and Processes | Limitation of Harm					ID.BE, ID.SC, ID.BE-P, ID.DE-P	ID.BE-1, ID.SC-1, ID.SC-2, ID.SC-3, ID.BE-P1, ID.DE-P1, ID.DE-P2, ID.DE-P3
SR-3(3)	Supply Chain Controls and Processes | Sub-tier Flow Down					ID.BE, ID.SC, ID.BE-P, ID.DE-P	ID.BE-1, ID.SC-1, ID.SC-2, ID.SC-3, ID.BE-P1, ID.DE-P1,

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
							ID.DE-P2, ID.DE-P3
SR-4	Provenance					ID.DE-P, CM.AW-P	ID.DE-P1, CM.AW-P6
SR-4(1)	Provenance | Identity					ID.DE-P, CM.AW-P	ID.DE-P1, CM.AW-P6
SR-4(2)	Provenance | Track and Trace					ID.DE-P, CM.AW-P	ID.DE-P1, CM.AW-P6
SR-4(3)	Provenance | Validate as Genuine and Not Altered					ID.DE-P, CM.AW-P	ID.DE-P1, CM.AW-P6
SR-4(4)	Provenance | Supply Chain Integrity — Pedigree					ID.DE-P, CM.AW-P	ID.DE-P1, CM.AW-P6
SR-5	Acquisition Strategies, Tools, and Methods		x	x	x	ID.SC, ID.DE-P	ID.SC-1, ID.SC-2, ID.SC-3, ID.DE-P1, ID.DE-P2, ID.DE-P3
SR-5(1)	Acquisition Strategies, Tools, and Methods | Adequate Supply					ID.SC, ID.DE-P	ID.SC-1, ID.SC-2, ID.SC-3, ID.DE-P1, ID.DE-P2, ID.DE-P3
SR-5(2)	Acquisition Strategies, Tools, and Methods | Assessments Prior to Selection, Acceptance, Modification, or Update					ID.SC, ID.DE-P	ID.SC-1, ID.SC-2, ID.SC-3, ID.DE-P1, ID.DE-P2, ID.DE-P3
SR-6	Supplier Assessments and Reviews			x	x	ID.SC, RS.AN, ID.DE-P	ID.SC-2, RS.AN-5, ID.DE-P2
SR-6(1)	Supplier Assessments and Reviews | Testing and Analysis					ID.SC, RS.AN, ID.DE-P	ID.SC-2, RS.AN-5, ID.DE-P2
SR-7	Supply Chain Operations Security						
SR-8	Notification Agreements		x	x	x	ID.DE-P	ID.DE-P3
SR-9	Tamper Resistance and Detection				x	DE.DP	DE.DP-2
SR-9(1)	Tamper Resistance and Detection | Multiple Stages of System Development Life Cycle				x	DE.DP	DE.DP-2
SR-10	Inspection of Systems or Components		x	x	x	DE.DP	DE.DP-2
SR-11	Component Authenticity		x	x	x		
SR-11(1)	Component Authenticity | Anti-counterfeit Training		x	x	x		
SR-11(2)	Component Authenticity | Configuration Control for Component Service and Repair		x	x	x		
SR-11(3)	Component Authenticity | Anti-counterfeit Scanning						
SR-12	Component Disposal		x	x	x	PR.IP, CT.DM-P	PR.IP-6, CT.DM-P5