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

February 23, 2024

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 **IAS_Governance@ed.gov**

APPROVAL

STEVEN
HERNANDEZ

Digitally signed by
STEVEN HERNANDEZ
Date: 2024.02.22
12:04:04 -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.
1.2	3/11/2022	Update Control Overlay SR-4 ED-01 and add Appendix B
1.3	3/10/2023	Annual review. Update broken links. Add footnote to HVA control reference in Section 2. Remove reference to SR-5 control overlay. Remove privacy baseline/SAOP reference from SR-1. Added SR-4 control overlay to address NIST SP 800-218 *Secure Software Development Framework, **(SSDF)*** considerations.
5.4	2/23/2024	Aligned document major version number to align with NIST SP 800-53 revision number. Clean up formatting and numbering throughout and update broken links. Section 2, Standards was updated to include the description of incorporating organizationally defined parameters (ODP) for controls that may be necessary from external control overlays (e.g., High Value Assets [HVA]). Updated Section 4, Acronyms as appropriate. Updated language in controls SR-01, SR-02, SR-02(01), SR-03(02), SR-03(03) ED-01, SR-04 ED-01, SR-04 ED-02, SR-04(02) ED-01, SR-04(03), SR-05, SR-05(02) ED-01, SR-10, SR-11(01), and SR-12. Added controls SR-05(02) ED-03, SR-11 ED-01, SR-11 ED-02, and SR-11 ED-03. Added control SR-04(02) ED-02 to the Moderate baseline. Added “leading zeros” to control identifiers in alignment with patch release of NIST SP 800-53 (Release 5.1.1) to applicable controls, enhancements, and overlays.

Table of Contents

1 INTRODUCTION

This governance document establishes U.S. Department of Education (Department or ED) information technology (IT) 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 (EO), Emergency Directives, Binding Operational Directives (BOD), and Department Administrative Communications System Directives (ACSD) and Handbooks. In doing so, these standards supersede any prior governance documentation establishing such standards.

1.1 Purpose

The Federal Information Security Modernization Act (FISMA)[1] and implementing governance 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.

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.

[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/wp-content/uploads/legacy_drupal_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

2 STANDARDS

The Department standards for IT system access controls 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 PUB 199 categorization level (e.g., Low [L], Moderate [M] and High [H]) is assigned to each requirement. This designator indicates a requirement applies to information systems categorized at that FIPS PUB 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 PUB 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[5] issued and maintained by the U.S. Department of Homeland Security (DHS), Cybersecurity & Infrastructure Security Agency (CISA). Systems that process federal tax information (FTI) must implement and comply with the Internal Revenue Service (IRS) Publication 1075[6], *Tax Information Security Guidelines for Federal, State and Local Agencies: Safeguards for Protecting Federal Tax Returns and Return Information.* Systems that are Federal Risk and Authorization Management Program (FedRAMP) authorized must implement and comply with the FedRAMP identified baselines[7].

Throughout the standard, there are controls captured that have not been scoped to any specific security or privacy baseline. This is intentional as all controls for identified external overlays and baselines (e.g., FedRAMP, IRS, HVA), that may apply to systems within the Department, have been incorporated into the standard. This ensures the organization defined parameters (ODPs) for controls within the Department have been clearly defined in a consistent manner.

This standard directly supports the Department's integration of the NIST Cybersecurity Framework (CSF) and NIST Privacy Framework (PF) by using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the Department's risk management processes. Refer to *APPENDIX A - BASELINE CONTROL PARAMETER SUMMARY* for a summary of controls by baseline and corresponding NIST CSF and NIST PF categories and subcategories.

2.1 SR-01 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

[5] HVA Control Overlay https://www.cisa.gov/resources-tools/resources/high-value-asset-control-overlay

[6] IRS Publication 1075 https://www.irs.gov/pub/irs-pdf/p1075.pdf

[7] FedRAMP baselines https://www.fedramp.gov/baselines/

of ED, or ED information as defined in ACSD-OCIO-004[8], *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 ACSD-OCIO-004, Cybersecurity Policy.

The Department CISO is 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.

[8] Also known as OCIO: 3-112.

2.2 SR-02 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; and

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-02(01) Supply Chain Risk Management Plan | Establish SCRM Team (L, M, H)

Establish a supply chain risk management team consisting of Supply Chain Risk Management (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’s 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; and

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-03 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-03(02) Supply Chain Controls and Processes | Limitation of Harm

Employ the following controls to limit harm from potential adversaries identifying and targeting the organizational supply chain:

a. Security controls may include:

   1. Supply Chain Redundancy – Procuring from or the ability to procure from several vendors to prevent supply issues;
   2. Scrutiny of Adversarial Products – Be aware of products manufactured, assembled, or shipped through adversarial countries and the possibility of tampering with controls to mitigate;
   3. Evaluation of Suppliers – Ensure the vendors used are well established, credible, and enable an acceptance level of fault tolerance; and/or
   4. Regular Assessments – Suppliers agree to cooperate with ED regarding risk assessment audits and inspections to ensure ongoing compliance in alignment with ED risk appetite and tolerance levels; and

b. In the event of an incident attributable to a failure in these security measures, the responsible party shall immediately take steps to limit the harm and prevent future incidents;

c. Notification shall occur for all impacted parties, as well as initiating an investigation, and the implementation of corrective and enhanced protocols as a result; and

d. ED and contractors agree to a collaborative approach in strengthening supply chain defenses and responding effectively to security threats. The contractor agrees to cooperate with ED regarding audits and inspections to ensure ongoing compliance.

2.3.2 SR-03(03) 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-03(03) ED-01 (L, M, H): Require Tier 1 (prime) contractors to include processes within risk management plans and Service Level Agreements (SLAs) to ensure sub-tier contractors implement SR-3(b), SR-5, and SR-8 controls.

2.4 SR-04 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-04 ED-01 (M, H): Obtain from software producers, artifacts that demonstrate conformance to secure software development practices, as needed, and provide artifacts obtained to the ICT SCRM Team. This activity is associated with the Secure Software Development Framework (SSDF) attestation and supporting artifacts to include the Software Bill of Materials (SBOM).

a. Determine if a SBOM is required as part of the overall SSDF attestation with other supporting artifacts, based upon the criticality of the software as defined in OMB M-21-30, *Protecting Critical Software Through Enhanced Security Measures*[9] or when necessary to manage risk. If required, the SBOM shall be retained by ED, unless the software producer posts it publicly and provides a link to that posting to the agency. SBOMs must be generated in one of the data formats defined by the National Telecommunications and Information Administration (NTIA) in Appendix B[10] or successor guidance as published by the Cybersecurity and Infrastructure Security Agency.

b. Consider reciprocity of SBOM and other artifacts from software producers that are maintained by other Federal agencies, based on direct applicability and currency of the artifacts.

c. Determine if artifacts, including the SBOM, are supporting the claim of software producers following the secure software development framework. As these are necessary to evaluate and manage risk from software producers.

Control Overlay SR-04 ED-02 (M, H): Protect non-public provenance data from unauthorized access, modification, and deletion.

2.4.1 SR-04(01) 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-04(01) ED-01 (H, M): 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-04(02) Provenance | Track and Trace (Control Overlay)

Establish and maintain unique identification of the following systems and critical system components for tracking through the supply chain: all hardware components.

Control Overlay SR-04(02) ED-01 (H): Label all hardware using serial numbers or radio frequency identification tags.

[9] OMB M-21-30, Protecting Critical Software Through Enhanced Security Measures

[10] National Telecommunications and Information Administration (NTIA) in Appendix B

Control Overlay SR-04(02) ED-02 (M, H): Report shipping delays or lost inventory to the ICT SCRM Team.

2.4.3 SR-04(03) Provenance | Validate as Genuine and Not Altered

Employ the following controls to validate that the system or system component received is genuine and has not been altered:

a. All hardware and software brought into the environment must be certified as genuine and unaltered from original state by the supplier;

b. Supplier guarantees all products are sourced directly from authorized manufacturers or distributors and have not been modified in any way;

c. Supplier shall provide adequate documentation to confirm authenticity and integrity of the products;

d. When a product is found not to be genuine and/or compliant with ED standards, the supplier, at their own expense shall promptly replace the affected product with genuine and compliant ones and shall be liable for any direct damages associated with the breach of the guarantee; and

e. The supplier agrees to cooperate with ED regarding counterfeit audits and inspections to ensure ongoing compliance.

2.5 SR-05 Acquisition Strategies, Tools, and Methods (L, M, H)

Employ the following acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks: Contractor attestation of conformance to current version of NIST SP 800-161, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* and Section 889 of the FY 2019 National Defense Authorization Act (NDAA) Part B[11]; Contractor reporting of supply chain cyber incidents to ED Security Operations Center (EDSOC); Contractor compliance with Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*; and ED ICT SCRM stakeholder training.

2.5.1 SR-05(02) 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-05(02) ED-01 (L, M, H): Evaluate the SSDF attestation, artifacts, and SBOM prior to the use of software, as required.

Control Overlay SR-05(02) 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.

[11] Section 889

Control Overlay SR-05(02) ED-03 (L, M, H): Conduct hash check against software packages and the software vendor for hash matching prior to installation and use inside of the ED environment.

2.6 SR-06 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-06(01) 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-06(01) ED-01 (M, H): Conduct supplier risk assessments in accordance with the ICT supply chain risk assessment schedule.

2.7 SR-08 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-09 Tamper Resistance and Detection (H)

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

2.8.1 SR-09(01) 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 and 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. Information System Owners, Information System Security Officers or other authorized system stakeholders, including contractor personnel, 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 SSDF attestation, artifacts, and 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.

Control Overlay SR-11 ED-01 (L, M, H): Follow ICT SCRM Team guidance/processes for detecting potential counterfeit devices.

Control Overlay SR-11 ED-02 (L, M, H): Conduct physical inspections of incoming hardware for indicators of counterfeit and/or tampering.

Control Overlay SR-11 ED-03 (L, M, H): Verify hash(es) on all incoming software against authoritative source (vendor or main provider), when possible.

2.10.1 SR-11(01) Component Authenticity | Anti-counterfeit Training (L, M, H)

Train, Information System Owners, Information System Security Officers, and others responsible for hardware and software inventories to detect counterfeit system components (including hardware, software, and firmware).

2.10.2 SR-11(02) 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) 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

Acronym	Definition
ACSD	Administrative Communications System Directives
BOD	Binding Operational Directive
CIO	Chief Information Officer
CISA	Cybersecurity & Infrastructure Security Agency
CISO	Chief Information Security Officer
CM.AW-P	Data Processing Awareness
CM-P	Communicate-P
CNSSI	Committee on National Security Systems Instruction
CO	Contracting Officer
COR	Contracting Officer's Representative
CSF	Cybersecurity Framework
CT.DM-P	Data Processing Management
CT-P	Control-P
DE	Detect
DE.DP	Detection Processes
Department	U.S. Department of Education
DHS	U.S. Department of Homeland Security
ED	U.S. Department of Education
EDSOC	ED Security Operations Center
EO	Executive Order
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
FTRI	Federal Tax Return Information
FY	Fiscal Year
GRP	Governance, Risk and Policy
GV.MT-P	Monitoring and Review
GV.PO-P	Governance Policies, Processes, and Procedures
GV-P	Govern-P
H	High
HVA	High Value Asset
IAS	Information Assurance Services
ICT	Information and Communications Technology
ID	Identify
ID.BE	Business Environment
ID.BE-P	Business Environment
ID.DE-P	Data Processing Ecosystem Risk Management
ID.GV	Governance
ID.SC	Supply Chain Risk Management
ID-P	Identify-P
IRS	Internal Revenue Service
ISCM	Information Security Continuous Monitoring
ISO	Information System Owner
ISSO	Information System Security Officer

Acronym	Definition
IT	Information Technology
L	Low
M	Moderate
MP	Media Protection Family
NDAA	National Defense Authorization Act
NIST	National Institute of Standards and Technology
NTIA	National Telecommunications and Information Administration
OCIO	Office of the Chief Information Officer
ODP	Organizationally Defined Parameters
OMB	Office of Management and Budget
P	Privacy
PF	Privacy Framework
PO	Principal Office
POA&M	Plan of Actions and Milestones
PR	Protect
PR.IP	Information Protection Processes and Procedures
PUB	Publication
RAF	Risk Acceptance Form
RS	Respond
RS.AN	Analysis
SAOP	Senior Agency Official for Privacy
SBOM	Software Bill of Materials
SCRM	Supply Chain Risk Management
SLA	Service Level Agreement
SP	Special Publication
SPDX	Software Package Data Exchange
SSDF	Secure Software Development Framework

APPENDIX A - BASELINE CONTROL PARAMETER SUMMARY

The applicability for each baseline control parameter is shown below.

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and PF Category	CSF and PF Subcategory
SR-01	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-02	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-02(01)	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-03	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-03(01)	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-03(02)	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,

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and PF Category	CSF and PF Subcategory
							ID.DE-P2, ID.DE-P3
SR-03(03)	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, ID.DE-P2, ID.DE-P3
SR-04	Provenance					ID.DE-P, CM.AW-P	ID.DE-P1, CM.AW-P6
SR-04(01)	Provenance | Identity					ID.DE-P, CM.AW-P	ID.DE-P1, CM.AW-P6
SR-04(02)	Provenance | Track and Trace					ID.DE-P, CM.AW-P	ID.DE-P1, CM.AW-P6
SR-04(03)	Provenance | Validate as Genuine and Not Altered					ID.DE-P, CM.AW-P	ID.DE-P1, CM.AW-P6
SR-04(04)	Provenance | Supply Chain Integrity — Pedigree					ID.DE-P, CM.AW-P	ID.DE-P1, CM.AW-P6
SR-05	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-05(01)	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-05(02)	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-06	Supplier Assessments and Reviews			X	X	ID.SC, RS.AN, ID.DE-P	ID.SC-2, RS.AN-5, ID.DE-P2
SR-06(01)	Supplier Assessments and Reviews | Testing and Analysis					ID.SC, RS.AN, ID.DE-P	ID.SC-2, RS.AN-5, ID.DE-P2
SR-07	Supply Chain Operations Security						
SR-08	Notification Agreements		X	X	X	ID.DE-P	ID.DE-P3
SR-09	Tamper Resistance and Detection				X	DE.DP	DE.DP-2

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and PF Category	CSF and PF Subcategory
SR-09(01)	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(01)	Component Authenticity | Anti-counterfeit Training		X	X	X		
SR-11(02)	Component Authenticity | Configuration Control for Component Service and Repair		X	X	X		
SR-11(03)	Component Authenticity | Anti-counterfeit Scanning						
SR-12	Component Disposal		X	X	X	PR.IP, CT.DM-P	PR.IP-6, CT.DM-P5

APPENDIX B – SBOM MINIMUM REQUIREMENTS

The minimum data requirements required by SR-4 and defined by the NTIA are documented in the table below.

NTIA Field	NTIA Description	Software Package Data Exchange (SPDX) 2.2.1 Field
Supplier Name	The name of an entity that creates, defines, and identifies components	Package Supplier
Component Name	Designation assigned to a unit of software defined by the original supplier	Package Name
Version of the Component	Identifier used by the supplier to specify a change in software from a previously identified version	Package Version
Other Unique Identifiers	Other identifiers that are used to identify a component, or serve as a look-up key for relevant databases	Package SPDX Identifier
Dependency Relationship	Characterizing the relationship that an upstream component X is included in software Y	Relationship
Author of SBOM Data	The name of the entity that creates the SBOM data for this component	Creator
Timestamp	Record of the date and time of the SBOM data assembly	Created