Standards Crosswalk
ISO 20243 & NIST 800-161

NASA Solutions for Enterprise-Wide Procurement

Executive Sponsor: Theresa Kinney (NASA)
Project Lead: Alexander Marshall (NASA SEWP)
Team Members: Demetrius Davis (MITRE), John Cofancesco (Fortress), Kristina Johnson (CISCO), Jon Johnson (NASA SEWP), Kiersten Patton (ATARC), Kim Reinke (Redhorse Corp.), Robert Salvia (Fortress), Tom Suder (ATARC), Michael Vande Woude (DHS, Consultant), Carol Woody (CMU SEI), Liza Zellers (Redhorse Corp.)

June 2021

EXECUTIVE SUMMARY

Supply Chain Risk Management (SCRM) regarding IT and government operations has emerged quickly as a matter of critical national and geo-political importance. The federal government has been taking direct actions to help secure their Information and Communication Technology (ICT) and Audio Visual (AV) assets that enter the government's federal infrastructure. Because digital assets and information are relied upon by everyone in our nation, efforts are underway to require vendors, who serve the federal government, to increase their efforts in securing the assets that are contained and transferred within our infrastructure.

There appears to be abundant confusion as this topic has emerged, since it appears to blend traditional supply chain management practices with cyber-hygiene elements into a single approach. Confusion over what to do, by whom, and for what purposes is still being made clear, as agency leaders, mission and business owners, and system owners look for ways to help shore up what they need to within their practices.

NASA SEWP has been working on Supply Chain Risk Management issues for over 20 years as they have maintained a buying platform that every agency uses to procure their ICT needs, and many of the principles and practices of SCRM are baked into the program's DNA. As members of the Open Group, they helped develop the first ISO standards dedicated to SCRM. As a member of the government acquisition community serving federal technology buyers, the program brought together a team of SCRM Subject Matter Experts to help provide clarity to some of what many find very confusing, and to identify actionable efforts that agency personnel can take today to account for SCRM within their processes, workflows, and requirements.

The primary question that the team asked was, "Whether commercial standards for SCRM could be used by federal buyers to account for part of what is required in existing NIST documentation?" This is an important initial question as OMB Circular NO.A-119 states "All federal agencies *must* use voluntary consensus standards in lieu of government-unique standards in their procurement and regulatory activities, except where inconsistent with law or otherwise impractical."[1] In fact, NIST stated "there are a surprising number of standards and guidelines for supply chain risk management" as they have identified ISO 20243 for acceptable use for help protecting the Cyber Supply Chain.[2] So this effort was to investigate how well, and to what extent, these standards applied for federal use.

Although appearing as a simple yes or no question, the exercise of doing a specific mapping of those standards and the applicable federal standards, including NIST 800-161, NIST IR 7622, DOD 5000.90, and NIST 800-161rev.1, produced surprising outcomes. This simple question resulted in a greater understanding of the supply chain dialogue itself, and why there may be confusion. There are more opportunities to create greater clarity and guidance for what buyers of high-impact systems need to account for from a cyber and supplier perspective, and we hope the following analysis provides a step in that direction.

---

[1] United Stated. Office of Management and Budget. OMB Circular NO.A-119. Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities. [Washington, D.C.]: Executive Office of the President, Office of Management and Budget.

[2] National Institute of Standards and Technology. Best Practices in Cyber Supply Chain Risk Management Conference Materials. Cyber Supply Chain Standards Mapping and Roadmap. https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-SCRM-Standards-Mapping.pdf

THE BACKGROUND

Supply Chain Risk Management (SCRM) is a topic of critical importance, reflected in federal legislation and policy. The Federal Acquisition Security Act of 2018, Section 889 of the 2019 National Defense Authorization Act, and the Biden Administration's Supply-Chain executive orders all point toward a continued focus. Federal agencies (as well as the industry base that works with, and supports, the federal government) have recently been required to take actions associated with Section 889, Cybersecurity Maturity Model Certification (CMMC), and the GAO Report on current SCRM practices as outlined in NIST-161. These are forthcoming actions and recommendations that will emerge from the studies required of the Biden Administration's executive orders on the Buy America Act, SCRM, and Cybersecurity, as well as forthcoming action and activities that emerge from the Federal Acquisition Security Council.

On December 2020, the Government Accountability Office (GAO) released a report, "Information Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks"[3]. That report states that agencies are required to "develop organizational ICT SCRM requirements for suppliers" and "develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment." Within this report to Congress, GAO assesses the current state of federal ICT SCRM practices at the 24 CFO Act Agencies[4] and how they have been executing the SCRM functions found within existing practices and legislation. These practices are anchored in existing guidance and legislation such as: the Federal Information Security Management Act of 2002 (FISMA); the Cyber Security Enhancement Act of 2014; a variety of NIST Special Publications involving Cybersecurity, Information Management, Identity Management, Risk Management and Supply Chain Management; and a variety of Executive Orders and OMB guidance.

The primary publication relevant to SCRM in the GAO assessment is NIST Special Publication 800-161 "Supply Chain Risk Practices for Federal Information Systems and Organizations."[5] This publication outlines the recommended SCRM-related activities federal agencies should take; some of which are activities required by agency leadership (accounting for a SCRM strategy for the agency), activities required by mission/business owners (accounting for SCRM's consideration within mission execution), and activities required by system owners (accounting for tactical SCRM considerations to account for system risk).

The activities recommended by NIST 161 include over 150 identified controls and control enhancements, and are broken down into particular practice domains: Information Security, Information Management, Identity Management, Risk Management, Supply Chain Management, and Procurement Management.[6]

The GAO report indicated that agencies are still working towards applying many of the NIST 161 recommended activities and need additional guidance on where the recommendations are applicable (e.g.

---

[3] Government Accountability Office. (2020). Information Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks. (GAO Publication No. 21-171). Washington, D.C.: https://www.gao.gov/assets/gao-21-171.pdf

[4] CFO Act Agencies are those defined by the Chief Financial Officer Act of 1990 (Pub. Law 101-576). More information can be found at https://www.cfo.gov/

[5] National Institute of Standards and Technology. (2015). Supply Chain Risk Management Practices for Federal Information Systems and Organizations. (NIST SP 800-161). Washington, D.C.: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf

[6] These controls can be found in the appendix.

high-impact systems as defined by FIPS 199), and how to include and execute those recommendations in agency operations.

NASA SEWP

Although SCRM may be relatively new to many, it is not for the team at NASA SEWP. In the early 1990's NASA SEWP became involved in X/Open[7], an early international IT open standards with an initial emphasis on UNIX-based systems. X/Open evolved into The Open Group[8], and NASA SEWP continued their involvement. In 2008, NASA SEWP and the Department of Defense worked with The Open Group through The Open Group Trusted Technology Forum[9] to help create the first international standards for Supply Chain Risk Management. The result was the creation of ISO/IEC 20243-1:2018 (O-TTPS)[10] - a set of guidelines, requirements, and recommendations that address specific threats to the integrity of Commercial Off-The-Shelf (COTS) ICT products within aspects of the product life cycle, and the standards carry a particular focus on "maliciously tainted and counterfeit products." NASA SEWP continues to serve on the organization's Governing Board and the Open Trusted Technology Forum.

SCRM standards and practices are program, and platform, features for SEWP. Currently nearly 50 NASA SEWP contract holders hold ISO 20243 certification. NASA SEWP employs various SCRM practices within their operations including: notating at the line level the TAA (Trade Agreement Act) status; capturing and displaying parent company affiliations (including the parent company name and address) for all manufacturer and service providers; employing a broad and verifiable process to clearly notate resellers who are approved by the original manufacturer; and employing practices that give CIO level visibility and control through "cleared catalogs" for products that are vetted and approved for agency acquisition.

As SCRM has emerged as a primary topic in the federal discourse and the GAO specifically noting the need to do more in this area, the SEWP experience and current processes lends itself to a natural series of questions. For example: Does ISO 20243 satisfy specific elements required or recommended through NIST SP 800-161? If so, what are they exactly? Can the ISO 20243 standard be used as a tool for agencies to assist in SCRM related processes? If so, how?

THE CHALLENGE QUESTION

These are the central questions that this document is focused on clarifying:

To what extent are ISO 20243 standards applicable to NIST 800-161? Can these two standards and guidelines be mapped as to how they complement and/or contradict one another? To what extent can the ISO 20243 standards be used by agency buyers to help fulfill their obligations associated with NIST 800-161?

---

[7] Wikipedia Contributors. (2020, May 29). In *Wikipedia, The Free Encyclopedia*. Retrieved 11:50, May 17, 2021, from, https://en.wikipedia.org/wiki/X/Open

[8] https://www.opengroup.org/

[9] https://www.opengroup.org/forum/trusted-technology-forum

[10] The Open Group. (2015). ISO/IEC 20243-1:2018. Information technology — Open Trusted Technology Provider Standard (O-TTPS) — Mitigating maliciously tainted and counterfeit products — Part 1: Requirements and recommendations. Burlington, MA

THE METHODOLOGY/PROCESS/APPROACH

SEWP leadership coordinated with government subject matter experts including those at NASA, the Department of Defense and the Department of Homeland Security along with the Advanced Technology Academic Research Center (ATARC) and industry representatives in order to develop, validate, vet, and assess the approach laid out below.

The first step was to delve into and dissect the ISO standards identified in ISO/IEC 20243-1:2018 "Information Technology – Open Group Trusted Technology Provider Standards (O-TTPS) – Mitigating maliciously tainted and counterfeit products – Part 1: Requirements and Recommendations" and 20243-1:2018 which contains "Part 2: Assessment procedure for the O-TTPS and ISO/IEC 20243-1:2018".

Part 1 of the ISO documentation provided the purpose and scope of the ISO standards, and broke the overall standard down logically into "Family" and "Group" areas, with associated definitions and terminology scope:

Family	Group
Supply Chain Security	Risk Management
	Physical Security
	Access Controls
	Employee and Supplier Security and Integrity
	Business Partner Security
	Supply Chain Security Training
	Information Systems Security
	Trusted Technology Components
	Secure Transmission and Handling
	Open Source Handling
	Counterfeit Mitigation
	Malware Detection
Product Development and Engineering	Software/Firmware/Hardware Design Process
	Configuration Management
	Well-defined Development/Engineering Method Process and Practices
	Quality and Test Management
	Product Sustainment Management
Secure Development and Engineering	Threat Analysis and Mitigation
	Run-time Protection Techniques
	Vulnerability Analysis and Response
	Product Patching and Remediation
	Secure Engineering Practices
	Monitor and Assess the Impact of Changes in the Threat Landscape

Each group had between 3-7 specific standards, indicated with an identifier and an accompanying description. Each individual standard broke down accordingly:

Family > Group > Group Definition > Standard > Standard Description

For example:

Supply Chain Security >

Risk Management > The management of supply chain risk around tainted and counterfeit components and products includes the identification, assessment, prioritization, and mitigation of corresponding business, technical, and operational risks.>

SC_RSM.01 > Changes to the threat landscape should be monitored by periodically reviewing industry security alerts/bulletins.

This information was captured, arranged and aggregated for simplicity as in the example below[11]:

Family	Group	Scope	Standard	Description
Supply Chain Security	Risk Management	The management of supply chain risk around tainted and counterfeit components and products includes the identification, assessment, prioritization, and mitigation of corresponding business, technical, and operational risks.	SC_RSM.01	Changes to the threat landscape should be monitored by periodically reviewing industry security alerts/bulletins.
Supply Chain Security	Risk Management		SC_RSM.02	Supply chain risk identification, assessment, prioritization, and mitigation shall be conducted.
Supply Chain Security	Risk Management		SC_RSM.03	The output of risk identification, assessment, and prioritization shall be addressed by a mitigation plan, which shall be documented.
Supply Chain Security	Risk Management		SC_RSM.04	The output of risk identification, assessment, and prioritization shall be addressed by a mitigation plan, which shall be followed routinely.
Supply Chain Security	Risk Management		SC_RSM.05	The mitigation plan should be reviewed periodically by practitioners, including management, and revised as appropriate.
Supply Chain Security	Risk Management		SC_RSM.06	Supply chain risk management training shall be incorporated in a provider's organizational training plan, which shall be reviewed periodically and updated as appropriate.

NIST 800-161

The team then approached NIST 800-161 in a similar manner with a thorough review of the purpose, goals, objectives, background, and guidance. The NIST standards made clear that this guidance was applicable to "high impact systems", a term-of-art defined within Federal Information Processing Standard Publication (FIPS) 199[12], Standards for Security Categorization of Federal Information and, Information Systems. The NIST publication includes a direct reference to the ISO standards, as well as a citation within the reference material.

[11] The complete list of these references are found in the appendix of this document.

[12] Radack, S. (2004). Federal Information Processing Standard (FIPS) 199. Standards for Security. ITL Bulletin. National Institute of Standards and Technology. Gaithersburg, MD. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=150427

The controls were then broken down and categorized within the NIST framework as had been done with the ISO Standards. Each individually identified control had:

- A "Control Family" which indicated the area of interests similar to the ISO "Families"
- A "Control Number" and "Control" similar to the ISO "Groups" and "Standard Number"
- A "Control Enhancement" which was a step or activity that goes beyond those anchored in the existing, applicable NIST standards
- An indication as to the responsible parties ("Tiers) within a federal agency (Organizational Leadership – Tier 1, Mission/Business Owners – Tier 2, and System Owners – Tier 3)
- NIST SP References

Individual standards found within NIST 800-161 were generally organized accordingly:

Family > Control Number > Control Title > Control Description & Requirements > Responsible Party/Tier > NIST Reference

For example:

Access Control > AC-1 > Access Control Policy and Procedures > Tiers 1, 2, 3 > NIST SP 800-12 & 800-100

As stated above, some controls also have a "Control Enhancement" that requires action in addition to what is already stated in the guidance or statute.

For example, Continuous Monitoring is required for Security Assessments and Authorizations. This is required of various NIST guidance for Risk Management and Information Security. In NIST 800-161 Continuous Monitoring has a Control Enhancement (Continuous Monitoring I Trend Analysis) that is addressed with "Supplemental ICT SCRM Guidance", and gives an indication of the responsible party (Tier 3 responsibility – System Owners).

As with the ISO standards, this information was captured, arranged, and aggregated for simplicity as in the example below [13]:

Family	Control No.	Control	Tier Responsibility	Sources
Access Control	AC-1	ACCESS CONTROL POLICY AND PROCEDURES	1, 2, 3	NIST 12, 100
Access Control	AC-2	ACCOUNT MANAGEMENT	2,3	
Access Control	AC-19	ACCESS CONTROL FOR MOBILE DEVICES	2,3	NIST 114, 124, 164, OMB M-06-16
Access Control	AC-20	USE OF EXTERNAL INFORMATION SYSTEMS	1, 2,3	FIPS 199
Awareness and Training	AT-1	SECURITY A&T POLICY AND PROCEDURES	1,2	NIST 12, 16, 50, 100

[13] The complete list of Access Controls are found in Appendix C of this document.

There were over 75 references to various NIST publications, DOD references, OMB memorandum, and other materials found within the controls that were also captured, arranged, and aggregated for simplicity as in the example below [14]:

NIST Reference	Title
800-16	Information Technology Security Training Requirements: a Role- and Performance-Based Model
800-23	Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products

NIST IR 7622

The Supply Chain Protection Control indicated NIST Interagency Report (IR) 7622 "National Supply Chain Risk Management Practices for Federal Information Systems"[15] as a referential anchor, so this document is included in the assessment and analysis. As with NIST 800-161, this document indicated particular activities suggested as practices as well as the responsible parties for these practices (federal executives, CIOs, CISOs, Contracting, Legal, and Mission/Business owners). The guidance also indicated suggested actions and activities for various roles within the supply chain exchange: The Acquirer (Government), the Integrator, and the Supplier.

The document outlined various practices that touched each part of a particular supply-chain activity. In some cases the Acquirer, the Integrator, and the Supplier would have a role to play. In other cases, there was only an activity required by one or two of the roles.

The requirements of suppliers in NIST IR 7622 were identified, captured, arranged, and aggregated for simplicity as in the example below:

NIST IR 7622 Supplier Requirements
Uniquely Identify Supply Chain Elements, Processes, and Actors
4.1.3 Suppliers –– General Requirements a) Apply unique identification requirements to delivered elements (e.g., serial numbers, date codes, license labels, etc.). b) Ensure that identification methods are sufficient to support provenance in the event of a supply chain issue or adverse supply chain event. c) Establish policies and procedures that require identification methods to support provenance in the event of a supply chain issue or adverse supply chain event. d) Define, design, and implement roles that limit privilege and create redundancy throughout the element life cycle to mitigate the risk of a single role being able to, intentionally or unintentionally, create adverse consequences. e) Require protection and safeguarding of authentication mechanisms.

[14] The complete list of these references are found in the appendix of this document.

[15] National Institute for Standards and Technology. (2012). Notional Supply Chain Risk Management Practices for Federal Information Systems. (NIST Interagency Report 7622). Washington DC. [online]. https://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7622.pdf

4.1.5 Suppliers – Technical Implementation Requirements None
4.1.8 Suppliers – Verification and Validation Requirements Report deficiencies discovered in critical elements (per acquirer/integrator) up the supply chain for corrective action to ensure that requirements for unique identification are fulfilled.

DOD 5000.90

The more recent DOD Instruction 5000.90 Cybersecurity for Acquisition Decision Authorities and Program Managers that became effective on December 31, 2020 were reviewed. Specifically the "SCRM Actions by Risk Tolerance Level" and PM actions requirements were identified, captured, and included for consideration:

SCRM Actions by Risk Tolerance Level	
High Risk Tolerance	High risk tolerance applies to simplified procurements, like computers at the Defense Commissary Agency. PMs should: • Exercise caution regarding products originating from sources with identified foreign ownership, control, or influence concerns. • Utilize approved products lists. • Maintain assurance through industry standards. • Balance risk against mission type.
Moderate Risk Tolerance	Moderate risk tolerance applies to structured procurements, like wireless networks at a forward deployed base. PMs should implement all previous strategies and: - Follow all requirements in DoDI 5200.44 and NIST SP 800-161; including: • Conducting criticality analysis. • Documenting in Program Protection Plan. • Sending requests on critical components/suppliers to the DIA SCRM TAC or other CI sources. • Flagging reports that come back critical, high, or select medium. Utilize the scoping and mitigations process to make mitigation decisions commensurate with risk.
Low Risk Tolerance	Low risk tolerance applies to engineered procurements, like industrial control systems in a tank. PMs should implement all previous strategies and: • Assess critical components. • Implement available countermeasures. • Utilize commercial assessment vendors, the Joint Federated Assurance Center, interagency and close and trusted international partners, national labs/FFRDCs, and intelligence and CI.
Very Low Risk Tolerance	Very low risk tolerance applies to assured procurements, like nuclear command and control systems. PMs should implement all previous strategies and: • Follow all requirements in DoDI 5200.44 and NIST SP 800-161; including: o Conducting criticality analysis. o Documenting in Program Protection Plan. o Sending requests on critical components/suppliers to the DIA SCRM TAC or other CI sources. o Flagging reports that come back critical, high, or select medium. Utilize the scoping and mitigations process to make mitigation decisions commensurate with risk.

Some of the requirements for Program Managers at the Department of Defense identified in DOD include:

> "Consider the source of products that may be supplied to fulfill program requirements, and seek alternatives to design of performance specifications or other program requirements that may necessitate the use of sources owned by, controlled by, or subject to the jurisdiction of a foreign adversary's government."

It also requires that the Program Managers "will maintain a complete list that shows, to the furthest extent possible:

- The ownership of commercial companies that currently do, or potentially will, supply (hardware, software, or firmware) components to the program
- Technology relationships with other companies that are known to already be under the influence or control of threat actors."

It also calls for Program Managers to:

- "Take action to manage supply chain risks, including those associated with foreign ownership, control, or influence concerns, commensurate with the risk tolerance level of the system or mission in question.
- Counter risks to and from a product by applying a framework for cybersecurity SCRM due diligence, that links supply chain risk tolerance with the importance of the systems purchased.
- Use assured suppliers or appropriate SCRM countermeasures for system elements that perform mission-critical functions."

THE ANALYSIS

By breaking down each individual standard document into their component controls or activities, the process of cross referencing drew out the overlap of requirements, and also resulted in an unanticipated outcome that could help frame future conversations.

One cause of confusion in current SCRM discussions is determining the boundaries between traditional supply chain management and the cyber-hygiene efforts that underpin most of the dialog. By organizing the information associated with NIST 161, the additional NIST control references were categorized between the domains. The NIST references found within each control were related to one of the following domains: Information Security, Information Management, Identity Management, Risk Management, Supply Chain Management, and Procurement Management.

Each NIST reference was tagged and color coded to a particular domain as in the below example:

NIST Reference	Title	Category
800-12	An Introduction to Information Security	Information Security
800-30	Guide for Conducting Risk Assessments	Risk Management
800-92	Guide for Security Log Management	Information Management
800-116	Guidelines for the Use of PIV Credentials	Identity Management
OMB M-07-08	Ensuring New Acquisitions Include Common Security Configurations	Procurement Management
NIST IR 7622	Notional Supply Chain Risk Management Practices for Federal Information Systems	Supply Chain Management

The NIST references were then cross referenced to categorize the controls found within NIST 161 into similar domains and color coded similar to the sample table below:

Family	Control No.	Control	Tier Responsibility	Sources						
Security Assessments and Authorizations	CA-2	SECURITY ASSESSMENTS	2, 3	NIST 37	NIST 39	NIST 53	NIST 115	NIST 137	EO 1358	FIPS 199
Security Assessments and Authorizations	CA-6	SECURITY AUTHORIZATION	1, 2, 3	NIST 37	NIST 137	M-11-33	A-130			
Identification and Authentication	IA-1	IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES	1, 2, 3	NIST 12	NIST 63	NIST 73	NIST 76	NIST 78	NIST 100	FIPS 201
System and Service Acquisition Policy	SA-3	SYSTEM DEVELOPMENT LIFE CYCLE	1, 2,3	NIST 37				NIST 64		
System and Service Acquisition Policy	SA-12	SUPPLY CHAIN PROTECTION	1, 2,3	NIST 161				NIST IR 7622		

This validated the content analysis making it clear that the ISO standards were most closely associated with the Supply Chain Protection “Controls” and “Control Enhancements” found within the Supply Chain Protection controls, and tagged to NIST 7622 and NIST 800-161 as the only corresponding references:

Enhancement No.	Supply Chain Protection Control Enhancements	Tier
SA-12 (1)	SUPPLY CHAIN PROTECTION | ACQUISITION STRATEGIES / TOOLS / METHODS	2, 3
SA-12 (2)	SUPPLY CHAIN PROTECTION | SUPPLIER REVIEWS	2, 3
SA-12 (5)	SUPPLY CHAIN PROTECTION | LIMITATION OF HARM	2, 3
SA-12 (7)	SUPPLY CHAIN PROTECTION | ASSESSMENTS PRIOR TO SELECTION / ACCEPTANCE / UPDATE	2, 3
SA-12 (8)	SUPPLY CHAIN PROTECTION | USE OF ALL-SOURCE INTELLIGENCE	2, 3
SA-12 (9)	SUPPLY CHAIN PROTECTION | OPERATIONS SECURITY	2, 3
SA-12 (10)	SUPPLY CHAIN PROTECTION | VALIDATE AS GENUINE AND NOT ALTERED	2, 3
SA-12 (11)	SUPPLY CHAIN PROTECTION | PENETRATION TESTING / ANALYSIS OF ELEMENTS, PROCESSES, AND ACTORS	2, 3
SA-12 (12)	SUPPLY CHAIN PROTECTION | INTER-ORGANIZATIONAL AGREEMENTS	2, 3
SA-12(13)	SUPPLY CHAIN PROTECTION | CRITICAL INFORMATION SYSTEM COMPONENTS	2, 3
SA-12(14)	SUPPLY CHAIN PROTECTION | IDENTITY AND TRACEABILITY	2, 3
SA-12 (15)	SUPPLY CHAIN PROTECTION | PROCESSES TO ADDRESS WEAKNESSES OR DEFICIENCIES	

Each individual control enhancement was reviewed and compared to the ISO controls to determine if the ISO controls met the need found within the control enhancement. In this scheme, the color code was green, yellow, and red to indicate whether the Supply Chain Protection need was met, partially met, or not met by the ISO standards as in this sample below:

Supply Chain Protection
SUPPLY CHAIN PROTECTION | ACQUISITION STRATEGIES / TOOLS / METHODS
SUPPLY CHAIN PROTECTION | SUPPLIER REVIEWS
SUPPLY CHAIN PROTECTION | LIMITATION OF HARM
SUPPLY CHAIN PROTECTION | ASSESSMENTS PRIOR TO SELECTION / ACCEPTANCE / UPDATE
SUPPLY CHAIN PROTECTION | USE OF ALL-SOURCE INTELLIGENCE
SUPPLY CHAIN PROTECTION | OPERATIONS SECURITY
SUPPLY CHAIN PROTECTION | VALIDATE AS GENUINE AND NOT ALTERED
SUPPLY CHAIN PROTECTION | PENETRATION TESTING / ANALYSIS OF ELEMENTS, PROCESSES, AND ACTORS
SUPPLY CHAIN PROTECTION | INTER-ORGANIZATIONAL AGREEMENTS
SUPPLY CHAIN PROTECTION | CRITICAL INFORMATION SYSTEM COMPONENTS
SUPPLY CHAIN PROTECTION | IDENTITY AND TRACEABILITY
SUPPLY CHAIN PROTECTION | PROCESSES TO ADDRESS WEAKNESSES OR DEFICIENCIES

The requirements within NIST 7622 were reviewed and compared to the recommendation made by the supplier role requirement in the ISO standards and map any overlap. This was also color coded where the color green indicated a direct map between the standards. This provides a qualitative and quantitative assessment of the standards and their mapping similar to the sample table below:

NIST IR 4622 Standard
Uniquely Identify Supply Chain Elements, Processes, and Actors
4.1.3 Suppliers -– General Requirements
4.1.8 Suppliers – Verification and Validation Requirements
Establish and Maintain the Provenance of Elements, Processes, Tools, and Data
4.3.3 Suppliers – General Requirements
4.3.5 Suppliers – Technical Implementation Requirements
4.3.8 Suppliers – Verification and Validation Requirements
Manage Disposal and Final Disposition Activities throughout the System or Element Life Cycle
4.10.3 Suppliers - General Requirements
4.10.5 Suppliers - Technical Implementation Requirements
4.10.8 Suppliers - Verification and Validation Requirements

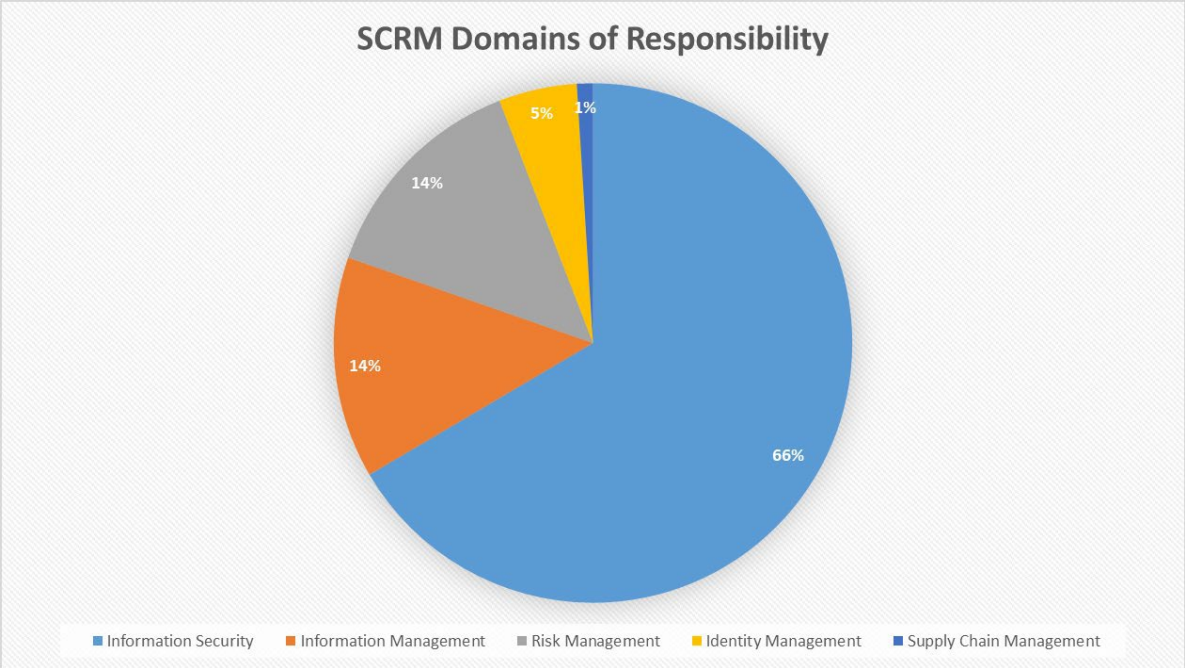
DOD 5000.90 was assessed textually to determine if the ISO standards: a) enhanced the ability for the DOD to execute their SCRM acquisition policies; b) supported the ability for DOD to execute their SCRM acquisition policies; c) contradicted the ability for DOD to execute their SCRM acquisition policies; or d) were not relevant and had no relationship.

THE RESULTS

Crosswalk Summary between ISO 20243 and NIST 800-161

The early textual review of the purpose, goals, and objectives indicated that NIST 800-161 covers a wide SCRM territory with recommended actions or considerations for a variety of stakeholders. The guidance is very clear that for high impact systems, agencies need to develop organizational ICT SCRM requirements for suppliers for inclusion in contracts that are tailored to the type of contract and the agencies business needs. It further required agencies to develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment. They recommend that agencies develop organizational procedures to detect ICT products that are counterfeit and have been compromised prior to their deployment to an operational environment. It was concluded that mapping the ISO standards to particular NIST controls, would provide a tool to Government acquisition teams in support of their due diligence with regards to SCRM. Such mapping would also assist the Acquisition teams to include within their requirements the appropriate NIST 800-161 requirements.

Review of the information broken down by subject domains and their corresponding, categorized reference material, identified the scope and breadth of the activities recommended by NIST 800-161. A breakdown of the domains indicate that the majority of federal agency requirements pertains to Information Security (66%), followed by Information Management (14%), Risk Management (14%), Identity Management (5%), and Supply Chain Management (1%). Below is the breakdown of the appropriate areas and domains for a comparative crosswalk to be easily targeted.



This analysis provided an assessment of the individual control groups to determine if a particular control requirement was:

1. Already addressed through existing NIST standards, agency activities, responsibilities or current and matters of practice; or
2. Required additional action on behalf of agency personnel in order to address a stated need.

The team then:

1. Categorized the action according to the SCRM Domain of Responsibility;
2. Validated that the Supply Chain Protection portion of the NIST Controls were the areas where the ISO standards would directly apply;
3. Reviewed each of the Supply Chain Protection Control enhancements;
4. Reviewed the purpose, content, and action associated with each enhancement;
5. Compared the enhancements to the ISO standards to determine if the standards directly met the stated need.

The results of this analysis are indicated in the table below:

NIST Control Number	NIST Control Enhancement	ISO Application Assessment
SA-12 (1)	SUPPLY CHAIN PROTECTION | ACQUISITION STRATEGIES / TOOLS / METHODS	This maps as ISO 20243 is a piece of what they require of an agency to consider.
SA-12 (2)	SUPPLY CHAIN PROTECTION | SUPPLIER REVIEWS	O-TTPS standards are an obvious tool or technique that can be leveraged for a portion of the risk that it is scoped for.
SA-12 (5)	SUPPLY CHAIN PROTECTION | LIMITATION OF HARM	ISO 20243 satisfies this requirement.
SA-12 (7)	SUPPLY CHAIN PROTECTION | ASSESSMENTS PRIOR TO SELECTION / ACCEPTANCE / UPDATE	ISO 20243 appears to satisfy this requirement.
SA-12 (8)	SUPPLY CHAIN PROTECTION | USE OF ALL-SOURCE INTELLIGENCE	Not a map - This is an agency requirement.
SA-12 (9)	SUPPLY CHAIN PROTECTION | OPERATIONS SECURITY	Not a map - but lightly compliments the intent of this control.
SA-12 (10)	SUPPLY CHAIN PROTECTION | VALIDATE AS GENUINE AND NOT ALTERED	ISO 20243 satisfies this requirement.
SA-12 (11)	SUPPLY CHAIN PROTECTION | PENETRATION TESTING / ANALYSIS OF ELEMENTS, PROCESSES, AND ACTORS	Not a direct map - but some elements contained in the standards. A government requirement that is not contradicted.
SA-12 (12)	SUPPLY CHAIN PROTECTION | INTER-ORGANIZATIONAL AGREEMENTS	ISO 20243 can satisfy this requirement.
SA-12 (13)	SUPPLY CHAIN PROTECTION | CRITICAL INFORMATION SYSTEM COMPONENTS	ISO 20243 satisfies this requirement.
SA-12 (14)	SUPPLY CHAIN PROTECTION | IDENTITY AND TRACEABILITY	ISO 20243 appears to satisfy this requirement.
SA-12 (15)	SUPPLY CHAIN PROTECTION | PROCESSES TO ADDRESS WEAKNESSES OR DEFICIENCIES	ISO 20243 satisfies this requirement.

Crosswalk Summary between ISO 20243 and NIST IR 7622

- The review of the supplier requirements, indicated the ISO standards ***directly met*** or complimented 50 of the 66 (75%) requirements and **potentially met** 59 of the 66 (89%) requirements.
- Note that the difference between “directly met” vs. “potentially met” would depend on interpretation of language used within the ISO or NIST descriptions in some instances.

The below table outlines the supplier requirements and a determination if the ISO standards meet those recommended requirements. The "# of Actions" column indicates the number of actions or activities required of a supplier in a particular area and tied to a specific reference number. The "Compliance Score" column notes to what extent the standards in ISO 20243 address the supplier requirements in NIST IR 7622.

For example, in the first instance there are 5 actions found in NIST IR 7622 Section 4.1.3 (Supplier Requirements – General) in the area of Uniquely Identifying Supply Chain Elements, Processes, and Actions. Looking specifically at each of those 5 actions and comparing them to the associated ISO Standards, "Are there standards that address the requirements? In this instance all 5 requirements of the suppliers are met by a corresponding standard in ISO 20243.

Area	Reference	Supplier Requirements	# of Actions	Compliance Score
Uniquely Identify Supply Chain Elements, Processes, and Actors	4.1.3	General	5	100%
Uniquely Identify Supply Chain Elements, Processes, and Actors	4.1.5	Verification and Validation	1	100%
Limit Access and Exposure within the Supply Chain	4.2.3	General	1	100%
Limit Access and Exposure within the Supply Chain	4.2.5	Technical Implementation	1	100%
Limit Access and Exposure within the Supply Chain	4.2.8	Verification and Validation	2	100%
Establish and Maintain the Provenance of Elements, Processes, Tools, and Data	4.3.3	General	5	80%
Establish and Maintain the Provenance of Elements, Processes, Tools, and Data	4.3.5	Technical Implementation	2	100%
Establish and Maintain the Provenance of Elements, Processes, Tools, and Data	4.3.8	Verification and Validation	2	100%
Share Information within Strict Limits	4.4.3	General	3	100%
Share Information within Strict Limits	4.4.5	Technical Implementation	3	100%
Share Information within Strict Limits	4.4.8	Verification and Validation	4	100%
Perform Supply Chain Risk Management Awareness and Training	4.5.3	General	1	100%
Perform Supply Chain Risk Management Awareness and Training	4.5.5	Technical Implementation	1	100%
Perform Supply Chain Risk Management Awareness and Training	4.5.8	Verification and Validation	1	100%
Use Defensive Design for Systems, Elements, and Processes	4.6.3	General	8	100%

Use Defensive Design for Systems, Elements, and Processes	4.6.5	Technical Implementation	8	87.5%*
Use Defensive Design for Systems, Elements, and Processes	4.6.8	Verification and Validation	2	100%
Strengthen Delivery Mechanisms	4.8.3	General	3	100%
Strengthen Delivery Mechanisms	4.8.5	Technical Implementation	5	80%**
Manage Disposal and Final Disposition Activities throughout the System or Element Life Cycle	4.10.3	General	2	100%*
Manage Disposal and Final Disposition Activities throughout the System or Element Life Cycle	4.10.5	Technical Implementation	4	25%
Manage Disposal and Final Disposition Activities throughout the System or Element Life Cycle	4.10.8	Verification and Validation	2	0%

(*) and (**) indicates that there are controls that are dependent on interpretation to achieve that compliance rating.

Crosswalk Summary between ISO 20243 and DOD 5000.90

The Department of Defense has an interest in monitoring certain elements of their supply chain, and for the past 4-5 years have been very assertive in instituting certain controls to help secure the information contained within the DOD and the Defense Industrial Base. The recent codification of DFAR rule 252.204-7021 to include the CMMC Requirements for designated procurements is an example of this trend. This December 31, 2020, DOD order outlined SCRM practices and activities required of their program managers. This guidance was included in our analysis, to determine if the ISO standards complimented, contradicted, or possibly augmented any of the DOD program manager requirements.

The DOD Order identified the appropriate actions associated with a particular risk tolerance ranging from High to Very Low tolerance. The ISO standards appeared to be closely associated with the desired actions for a High Tolerance Risk environment. DOD included more “best practice” guidance with these activities such as understanding ownership controls, using approved products lists, and leveraging applicable industry standards. ISO 20243 would be an example of an industry standard that could be applied along with the other measures required of program managers.

Aside from this one aspect, there was no directly attributable way to map the ISO standards to this DOD Instructional Letter. The ISO standard, however, could be leveraged by DOD as a complimentary feature.

NIST 800-161REV.1, The Biden Administration Executive Order & CISA

There is ample proof that the topic of SCRM in federal government is changing rapidly. While undergoing the final revisions for this analysis, in April 2021, the Cybersecurity and Infrastructure Security Agency (CISA), NIST, and the Department of Commerce released their publication on "Defending Against Software Supply Chain Attacks"[16], NIST released a 800-161 Rev.1 "Cyber Supply Chain Risk Management Practices for System and Organizations"[17], and in May 2021, the Biden Administration released the "Executive Order on Improving the Nation's Cybersecurity."[18] Each were also reviewed and considered.

CISA Publication

CISA's publication continues to advance their role in the federal C-SCRM conversation as they execute their mission and obligations to monitor U.S. Critical Infrastructure. The focus is on providing insights into the kind of threats that can affect the ICT supply chain, and supported by known events that bring real-time examples that ICT security professionals are already familiar with. CISA also makes recommendations of how suppliers are accounted for.

Examples include:

- Closely collaborating with key suppliers
- Knowing and managing critical components and suppliers
- Including suppliers in resilience and improvement activities
- Assessing and monitoring throughout the supplier relationship
- Using supplier certifications to account for risk

The CISA guidance is focused on the C-SCRM related primarily for software, therefore there is a limitation to the application of the ISO standards. The practices do, however, appear consistent with many of the principles that underlie the ISO standards, and are consistent with the general SCRM practices recommended by the NASA SEWP PMO.

Biden Administration E.O. 13873

This order, like the CISA guidance, focuses primarily on enhancing the software supply chain and supports CISA role and activities. As with the other executive orders referenced here, this requires a variety of activities from a number of federal agencies to consider security and contractual action to help secure the

[16] Cybersecurity and Infrastructure Security Agency. (2021). Defending Against Software Supply Chain Attacks. Washington, DC. [Online]. https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508_1.pdf

[17] National Institute for Standards and Technology. (2021). Cyber Supply Chain Risk Management Practices for System and Organizations. (NIST SP 800-161.rev.1). Washington DC. [Online]. https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/draft

[18] The White House. (May 12, 2021). Executive Order on Improving the Nation's Cybersecurity. (E.O. 13873). Washington DC. [Online]. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

country's infrastructure. Nothing in the ISO standards contradict what is called for in this initiative, and it could be a tool that suppliers and government use, however there is no direct correlation between the two at this time.

NIST SP 800-161 Rev.1

This document was reviewed and accounted for completely. There were notable changes proposed between NIST 800-161 and the April 2021 released revision, and an attempt was made to only note the changes and assess whether the ISO standards could still be used as a tool considering what was being proposed with this new version.

Major changes include:

- Use of C-SCRM as the term of art
- 61 additional controls
- The elimination of the Supply Chain Protection controls
- Acquisition Security Guidance
- A significantly expanded set of controls around the topic of "Program Management"
- Inclusion of PII control

We put this version through the same methodology described in the above section on the assessment of NIST 161. Although the controls lacked the same prior NIST Special Publications anchors used in the initial analysis, the control groups maintained their topical focus on matters of information security, information management, risk management, and identity management.

The overall impression from the team is that the ISO standards satisfy a portion of what is required of federal agencies in terms of some validation for supply chain controls within their operations, as a way to account for certain risks, to help protect against taint and counterfeit products entering an ICT supply chain. With this recent draft, however, it appears that the future efforts of the government, and demands made from industry, will be focused on that cyber aspect of the supply chain. Existing ISO standards can still be leveraged to support those efforts if used along with other practices such as those noted in the conclusion of this document. C-SCRM practices are still required to be accounted for by acquisition personnel with supply chain information sharing and monitoring as a noted practice required of the ISO standards, and C/SCRM training and awareness are part of what vendors are assessed on when applying for their certification.

The ISO standards appear to compliment what will be required of agency personnel to consider, but is one of many practices that the federal community will need to operationalize. The release of these standards usually indicate the beginning, not the end, of a conversation that involves industry and government. Although the changes appear to bring greater clarity to the scope and guidance found within NIST 800-161, a definitive statement as to how ISO standards fit with the requirements and recommendations in 800-161 Rev.1 would be premature at this time.

THE CONCLUSIONS, LIMITATIONS AND IMPLICATIONS

The team exercise led to a number of conclusions that could assist federal acquisition professionals apply existing means to partially satisfy requirements and recommendations of NIST SP 800-161 and NIST IR 7622. The team drew the following conclusions based on the textual analysis and above described methodology:

Conclusions

- The O-TTPS's ISO 20243 SCRM Standards for "maliciously tainted and counterfeit products" standards are consistent in purpose and intent with existing and emergent federal policy materials and guidelines that have been proposed or currently in draft format.
- The ISO 20243 SCRM Standards provides a measure of risk management agencies can use to satisfy certain portions of NIST 800-161 and NIST IR 7622.
- The ISO 20243 SCRM Standards map to between 75-89% of the supplier risk controls recommended in NIST IR 7622.
- The ISO 20243 SCRM Standards fully addresses 5 of the 12 Supply Chain Management Control Enhancements found in the existing NIST 800-161
- The ISO 20243 SCRM Standard satisfies 9 of the 12 Supply Chain Management Control Enhancements and compliments 2 of the remaining 3 controls found in the existing NIST 800-161.
- There is only one Supply Chain Management Control Enhancement Control in NIST 800-161 that ISO 20243 SCRM cannot satisfy and does not address.

Limitations

The scope of the O-TTPS ISO 20243 standard is particular to "maliciously tainted and counterfeit products". The standard is geared more to the manufacturing environment and managing the handoffs associated with manufacturing, distribution, and reselling.

Many of the contemporary concerns associated with SCRM pertain to the software development environment, and includes patching and updating of software and firmware. Many of the contemporary concerns also result in having cyber-capabilities that can "sniff" the network in order to determine the integrity of the system and their component parts. The ISO standard can help with communication accountability when a vulnerability becomes known, but the depth of visibility into the totality of the supply chain is not within the scope of these, or any commercial, standards beyond accepted DevSecOps practices.

These limitations are the gaps by which government and industry dialog can be centered in the federal SCRM conversation.

Implications

The Federal SCRM conversation is a complicated and confusing one. The standards that document requested actions by Agency Executive, Mission/Business Owners, and System Owners cover a number of domains. The appetite for controls at this point outpace the ability to control certain features of the ICT supply chain. Evidence of the challenges can be found within the December 2020 GAO report on Supply Chain Risk which was critical of the efforts government has taken to date. More clarity is needed in how to

leverage existing practices to begin mitigating risks. Weaving these practices together across the SCRM Domains of Responsibility will be a challenge.

To assist federal agencies address these needs, NASA SEWP and the team of SCRM experts assessed an existing standard that fits an area of this practice puzzle. There are additional SCRM practices available that can help agencies adhere to the NIST standards beyond the ISO standard, and more information on guidance, support, and practices are forthcoming once the required reviews are completed as a result of the Biden Administration E.O. on the Federal Supply Chain.

NASA SEWP has worked with the Department of Defense, Private Industry and International Standards Groups for almost 20 years on SCRM practices and standards. NASA SEWP includes O-TTPS's ISO 20243 standard as a buyer's option on the NASA SEWP acquisition platform. However, a direct correlation between the ISO standard and the controls and practices advocated by NIST was missing until now. As outlined in this paper, doing so validated our initial impression that the standard addresses some SCRM needs and can be leveraged by federal buyers to comply with recommended practices. The ISO standard can be applied throughout Government buying platforms utilizing articulated requirements.

The standard is limited and focused. It is not satisfactory to deal with the software vulnerabilities that exist as a result of the nature of international business practices. The standard is not inclusive of all activities that are advocated by SCRM professionals. For example, some basic practices that the program, and SCRM professionals, advocate for and can be immediately applied are:

1. **Capturing Vendor Relationships** – Every agency should know the relationship between entities, and that includes knowledge of the parent company or any other obfuscated ownership structure.
2. **'Authorized' resellers** – Authorized resellers are a common approach in the federal market, but the terminology is ill-defined or more precisely multi-defined. Industry's usage of this phrase ranges from a formal vetting process that can have significant supply chain risk mitigation; to a formal business process used primarily to reduce or eliminate competition and control pricing with no supply chain risk benefit; to having little to no actual meaning. The processes involved in verifying and assigning authorization are as varied as the meaning. Overemphasis of the term "Authorized Reseller" without proper context and verification and without accounting for the wide range of Industry practices in this area can cause more issues without reducing risk.
3. **Assessed and Cleared Product Catalogs** – CIOs require visibility and controls while also allowing for requirements-specific buying for particular mission needs. Catalogs, such as the NASA ICT Catalog for Cleared Technology, are a means to help create a static buying platform with dynamic capabilities to include emerging, capable, and secure technology.

The need for change and adaptation are a certainty in today's environment, and the NASA SEWP program looks forward to using its program's knowledge and expertise to help make sense of this issue for federal buyers so we can do our part in continuing to secure NASA and the federal government's supply chain. We hope this assessment will assist federal buyers in accounting for part of their SCRM responsibilities. If you have any questions please contact the NASA SEWP program by e-mailing help@sewp.nasa.gov

---

Appendix A: Table of ISO 20243 Standards

Jump back to footnote

The below table contains the list of ISO 20243 Standards developed by The Open Group that were considered as part of this review. Source information can be found here: The Open Group. (2015). ISO/IEC 20243-1:2018. Information technology — Open Trusted Technology Provider Standard (O-TTPS) — Mitigating maliciously tainted and counterfeit products — Part 1: Requirements and recommendations. Burlington, MA

Family	Group	Scope	Standard	Description
Supply Chain Security	Risk Management	The management of supply chain risk around tainted and counterfeit components and products includes the identification, assessment, prioritization, and mitigation of corresponding business, technical, and operational risks.	SC_RSM.01	Changes to the threat landscape should be monitored by periodically reviewing industry security alerts/bulletins.
Supply Chain Security	Risk Management		SC_RSM.02	Supply chain risk identification, assessment, prioritization, and mitigation shall be conducted.
Supply Chain Security	Risk Management		SC_RSM.03	The output of risk identification, assessment, and prioritization shall be addressed by a mitigation plan, which shall be documented.
Supply Chain Security	Risk Management		SC_RSM.04	The output of risk identification, assessment, and prioritization shall be addressed by a mitigation plan, which shall be followed routinely.
Supply Chain Security	Risk Management		SC_RSM.05	The mitigation plan should be reviewed periodically by practitioners, including management, and revised as appropriate.

Supply Chain Security	Risk Management		SC_RSM.06	Supply chain risk management training shall be incorporated in a provider's organizational training plan, which shall be reviewed periodically and updated as appropriate.
Supply Chain Security	Physical Security	Physical security procedures are necessary to protect development assets and artifacts, manufacturing processes, the plant floor, and the supply chain.	SC_PHS.01	Risk-based procedures for physical security shall be established and documented.
Supply Chain Security	Physical Security		SC_PHS.02	Risk-based procedures for physical security shall be followed routinely.
Supply Chain Security	Physical Security		SC_PHS.02	Risk-based procedures for physical security shall be followed routinely.
Supply Chain Security	Access Controls	Proper access controls are established for the protection of product-relevant intellectual property against the introduction of tainted and counterfeit components where applicable in the supply chain. Access controls can vary by type of intellectual property and over time, during the life cycle.	SC_ACC.01	Access controls shall be established and managed for product-relevant intellectual property, assets, and artifacts. Assets and artifacts include controlled elements related to the development/manufacturing of a provider's product.
Supply Chain Security	Access Controls		SC_ACC.02	Access controls established and managed for product-relevant intellectual property, assets, and artifacts shall be documented.
Supply Chain Security	Access Controls		SC_ACC.03	Access controls established and managed for product-

				relevant intellectual property, assets, and artifacts shall be followed routinely.
Supply Chain Security	Access Controls	Proper access controls are established for the protection of product-relevant intellectual property against the introduction of tainted and counterfeit components where applicable in the supply chain. Access controls can vary by type of intellectual property and over time, during the life cycle.	SC_ACC.04	Access controls established and managed for product-relevant intellectual property, assets, and artifacts should be reviewed periodically by practitioners, including management, and revised as appropriate.
Supply Chain Security	Access Controls		SC_ACC.05	Access controls established and managed for product-relevant intellectual property, assets, and artifacts shall employ the use of access control auditing.
Supply Chain Security	Employee and Supplier Security and Integrity	Background checks are conducted for employees and contractors whose activities are directly related to sensitive product supply chain activities. A Provider has a set of applicable business conduct guidelines for their employee and supplier communities. A	SC_ESS.01	Proof of identity shall be ascertained for all new employees and contractors engaged in the supply chain, except where prohibited by law.
Supply Chain Security	Employee and Supplier Security and Integrity		SC_ESS.02	Background checks should be conducted for employees and contractors whose activities are directly related to sensitive product supply chain activities (within reason given local customs and according to local law).

Supply Chain Security	Employee and Supplier Security and Integrity	Electronic Industry Citizenship Coalition (EICC) Code of Conduct.	SC_ESS.03	A set of business conduct guidelines applicable to its employees and contractors should exist, consistent with principles embodied in industry conduct codes such as the Electronic Industry Citizenship Coalition (EICC) Code of Conduct.
Supply Chain Security	Employee and Supplier Security and Integrity		SC_ESS.04	Business should be conducted in a manner consistent with principles embodied in industry conduct codes, such as the Electronic Industry Citizenship Coalition (EICC) Code of Conduct.
Supply Chain Security	Employee and Supplier Security and Integrity		SC_ESS.05	Periodic confirmation that suppliers are conducting business in a manner consistent with principles embodied in industry conduct codes, such as the Electronic Industry Citizenship Coalition (EICC) Code of Conduct, should be obtained.
Supply Chain Security	Business Partner Security	(This includes, for example, Suppliers, Integrators, Logistic Partners, Channel Partners, and Authorized Resellers.) Relevant business partners follow the recommended supply chain security best practice	SC_BPS.01	Supply chain security best practices (e.g., O-TTPS) shall be recommended to relevant business partners.
Supply Chain Security	Business Partner Security		SC_BPS.02	Legal agreements with business partners should reference applicable

		requirements specified by the O-TTPS. Periodic confirmation is requested that business partners are following the supply chain security best practices requirements specified by the O-TTPS.		requirements for supply chain security practices (e.g., O-TTPS).
Supply Chain Security	Business Partner Security		SC_BPS.03	The provider should periodically request confirmation that business partners are following the supply chain security best practice requirements specified by the O-TTPS.
Supply Chain Security	Supply Chain Security Training	Personnel responsible for the security of supply chain aspects are properly trained.	SC_STR.01	Training in supply chain security procedures shall be given to all appropriate personnel.
Supply Chain Security	Information Systems Security		SC_ISS.01	Supply chain data shall be protected through an appropriate set of security controls.
Supply Chain Security	Trusted Technology Components	Supplied components are evaluated to assure that they meet component specification requirements. Suppliers follow supply chain security best practices with regard to supplied components (e.g., O-TTPS).	SC_TTC.01	The quality of supplied components shall be assessed against the component specification requirements.
Supply Chain Security	Trusted Technology Components		SC_TTC.02	Counterfeit components shall not knowingly be incorporated into products.
Supply Chain Security	Trusted Technology Components		SC_TTC.03	Suppliers should be required to follow supply chain security best practices with regard to supplied components (e.g., O-TTPS).
Supply Chain Security	Trusted Technology Components		SC_TTC.04	Vulnerability responses to affected supplied components should be

				jointly managed with the supplier.
Supply Chain Security	Secure Transmission and Handling	Secure transmission and handling of assets and artifacts during delivery is needed to lower the risk of product tampering while in transit to their destination.	SC_STH.01	Secure transmission and handling controls shall be established and documented.
Supply Chain Security	Secure Transmission and Handling		SC_STH.02	Secure transmission and handling controls shall be designed to lower the risk of physical tampering with assets and artifacts that are physically transported.
Supply Chain Security	Secure Transmission and Handling		SC_STH.03	Secure transmission and handling controls shall be designed to lower the risk of tampering with assets and artifacts that are electronically transmitted.
Supply Chain Security	Secure Transmission and Handling		SC_STH.04	Secure transmission and handling controls shall be followed routinely.
Supply Chain Security	Secure Transmission and Handling		SC_STH.05	Secure transmission and handling controls should be reviewed periodically by practitioners, including management, and revised as appropriate.
Supply Chain Security	Secure Transmission and Handling		SC_STH.06	For assets and artifacts and related information that are considered to be high risk from the supply chain perspective, additional countermeasures, such as

				authenticity verification, should be employed.
Supply Chain Security	Secure Transmission and Handling		SC_STH.07	Methods of verifying authenticity and integrity of products after delivery should be available.
Supply Chain Security	Open Source Handling	Open Source components are managed as defined by the best practices within the O-TTPS for Product Development/ Engineering methods and Secure Development/Engineering methods.	SC_OSH.01	Open Source assets and artifacts should be managed as defined by the best practices within the O-TTPS for Product Development/Engineering methods and Secure Development/Engineering methods.
Supply Chain Security	Open Source Handling		SC_OSH.02	In the management of Open Source assets and artifacts, components sourced shall be identified as derived from well-understood component lineage.
Supply Chain Security	Open Source Handling		SC_OSH.03	In the management of Open Source assets and artifacts, components sourced shall be subject to well-defined acceptance procedures that include asset and artifact security and integrity before their use within a product.
Supply Chain Security	Open Source Handling		SC_OSH.04	For such sourced components, responsibilities for ongoing support and

				patching shall be clearly understood.
Supply Chain Security	Counterfeit Mitigation	Practices are deployed to manufacture, deliver, and service products that do not contain counterfeit components. Practices are deployed to control the unauthorized use of scrap from the hardware manufacturing process.	SC_CTM.01	Instances of counterfeit activity relating to products shall be reviewed and an appropriate response sent.
Supply Chain Security	Counterfeit Mitigation		SC_CTM.02	Proper disposal procedures upon end of life should be employed (e.g., clearing data from hard drives, rendering a PCB non-functional, etc.) to protect from re-use in counterfeit product.
Supply Chain Security	Counterfeit Mitigation		SC_CTM.03	Practices should be deployed to preclude the unauthorized (counter-indicated) use of scrap from the hardware manufacturing process.
Supply Chain Security	Counterfeit Mitigation		SC_CTM.04	Techniques shall be utilized as applicable and appropriate to mitigate the risk of counterfeiting, such as security labeling and scrap management techniques.
Supply Chain Security	Malware Detection	Practices are employed that mitigate as much as practical the inclusion of malware in	SC_MAL.01	One or more up-to-date malware detection tools shall be deployed as part of the code acceptance and development processes.

Supply Chain Security	Malware Detection	components received from suppliers and components or products delivered to customers or integrators.	SC_MAL.02	Malware detection techniques shall be used before final packaging and delivery (e.g., scanning finished products and components for malware using one or more up-to-date malware detection tools).
Product Development and Engineering	Software/Firmware/Hardware Design Process	Process that defines and documents how requirements are translated into a product design.	PD_DES.01	A process shall exist that assures the requirements are addressed in the design.
Product Development and Engineering	Software/Firmware/Hardware Design Process		PD_DES.02	Product requirements shall be documented.
Product Development and Engineering	Software/Firmware/Hardware Design Process		PD_DES.03	Product requirements should be tracked as part of the design process.
Product Development and Engineering	Configuration Management	A formal process and supporting systems exist which assure the proper management, control, and tracking of change to product development and manufacturing assets and artifacts.	PD_CFM.01	A documented formal process shall exist which defines the configuration management process and practices.
Product Development and Engineering	Configuration Management		PD_CFM.02	Baselines of identified assets and artifacts under configuration management shall be established.
Product Development and Engineering	Configuration Management		PD_CFM.03	Changes to identified assets and artifacts under configuration management shall be tracked and controlled.
Product Development and Engineering	Configuration Management		PD_CFM.04	Configuration management should be applied to build management and

		A formal process and supporting systems exist which assure the proper management, control, and tracking of change to product development and manufacturing assets and artifacts.		development environments used in the development/engineering of the product.
Product Development and Engineering	Configuration Management		PD_CFM.05	Access to identified assets and artifacts and supporting systems shall be protected and secured.
Product Development and Engineering	Configuration Management		PD_CFM.06	A formal process shall exist that establishes acceptance criteria for work products accepted into the product baseline.
Product Development and Engineering	Well-defined Development/Engineering Method Process and Practices	Development/engineering processes and practices are documented, and managed and followed across the life cycle.	PD_MPP.01	The development/engineering process as documented should be inclusive of development partners as defined by the governance process.
Product Development and Engineering	Well-defined Development/Engineering Method Process and Practices		PD_MPP.02	The development/engineering process shall be able to track, as appropriate, components that are proven to be targets of tainting or counterfeiting as they progress through the life cycle.
Product Development and Engineering	Quality and Test Management	Quality and test management is practiced as part of the product development/engineering life cycle.	PD_QAT.01	There shall be a quality and test product plan that includes quality metrics and acceptance criteria.

Product Development and Engineering	Quality and Test Management	Quality and test management is practiced as part of the product development/engineering life cycle.	PD_QAT.02	Testing and quality assurance activities shall be conducted according to the plan.
Product Development and Engineering	Quality and Test Management		PD_QAT.03	Products or components shall meet appropriate quality criteria throughout the life cycle.
Product Development and Engineering	Product Sustainment Management	Product support, release maintenance, and defect management are product sustainment services offered to acquirers while the product is generally available.	PD_PSM.01	A release maintenance process shall be implemented.
Product Development and Engineering	Product Sustainment Management		PD_PSM.02	Release maintenance shall include a process for notification to acquirers of product updates.
Product Development and Engineering	Product Sustainment Management		PD_PSM.03	Release maintenance shall include a product update process, which uses security mechanisms.
Product Development and Engineering	Product Sustainment Management		PD_PSM.04	A defect management process shall be implemented.
Product Development and Engineering	Product Sustainment Management		PD_PSM.05	The defect management process shall include: a documented feedback and problem reporting process.
Secure Development and Engineering	Threat Analysis and Mitigation	Threat analysis and mitigation identify a set of potential attacks on a particular product or system and describe how those attacks might be	SE_TAM.01	Product architecture and design shall be assessed against potential attacks to gain an understanding of the threat landscape.
Secure Development and Engineering	Threat Analysis and Mitigation		SE_TAM.02	Threat mitigation strategies for tainted and counterfeit products shall be

		perpetrated and the best methods of preventing or mitigating potential attacks.		implemented as part of product development.
Secure Development and Engineering	Threat Analysis and Mitigation		SE_TAM.03	Threat analysis shall be used as input to the creation of test plans and cases.
Secure Development and Engineering	Run-time Protection Techniques	Run-time protection techniques are considered part of a secure development/engineering method. This includes techniques to mitigate the exploitation of vulnerabilities. For example, run-time protection techniques help defend executable code against buffer overflow attacks, null pointers, etc.	SE_RTP.01	Run-time protection techniques as applicable to product architecture should be employed.
Secure Development and Engineering	Run-time Protection Techniques		SE_RTP.02	Run-time protection techniques should be included to mitigate the impact of vulnerabilities.
Secure Development and Engineering	Run-time Protection Techniques		SE_RTP.03	Run-time protection techniques should be included to protect executable code against memory space, buffer overflow attacks, and null pointers.
Secure Development and Engineering	Vulnerability Analysis and Response	Vulnerability analysis is the process of determining whether a product contains vulnerabilities and categorizing their potential severity.	SE_VAR.01	Techniques and practices for vulnerability analysis shall be utilized. Some techniques include: code review, static analysis, penetration testing, white/black box testing, etc.
Secure Development and Engineering	Vulnerability Analysis and Response		SE_VAR.02	The impact of published vulnerabilities to products and processes should be analyzed and mitigated.
Secure Development and Engineering	Vulnerability Analysis and Response		SE_VAR.03	A process shall exist for governing notification of newly discovered and

				exploitable product vulnerabilities.
Secure Development and Engineering	Vulnerability Analysis and Response		SE_VAR.04	Vulnerability analysis and response should feed into the processes for ongoing product development, product patching, and remediation.
Secure Development and Engineering	Product Patching and Remediation	A well-documented process exists for patching and remediating products. Priority is given to known severe vulnerabilities.	SE_PPR.01	There shall be a well-documented process for patching and remediating products.
Secure Development and Engineering	Product Patching and Remediation		SE_PPR.02	There should be a process for informing an acquirer of notification and remediation mechanisms.
Secure Development and Engineering	Product Patching and Remediation		SE_PPR.03	Remediation of vulnerabilities shall be prioritized based on a variety of factors, including risk.
Secure Development and Engineering	Product Patching and Remediation		SE_PPR.04	Documented development and sustainment practices should be followed when implementing product remediation.
Secure Development and Engineering	Secure Engineering Practices	Secure engineering practices are established to avoid common engineering errors that lead to exploitable product vulnerabilities.	SE_SEP.01	Secure coding practices shall be utilized to avoid common coding errors that lead to exploitable product vulnerabilities. For example, user input validation, use of appropriate compiler flags, etc.

Secure Development and Engineering	Secure Engineering Practices	Secure engineering practices are established to avoid common engineering errors that lead to exploitable product vulnerabilities.	SE_SEP.02	Secure hardware design practices (where applicable) shall be employed. For example, zeroing out memory and effective opacity.
Secure Development and Engineering	Secure Engineering Practices		SE_SEP.03	Training on secure engineering practices shall be provided to the appropriate personnel on a regular basis consistent with changing practices and the threat landscape.
Secure Development and Engineering	Monitor and Assess the Impact of Changes in the Threat Landscape	The threat landscape is monitored and the potential impacts of changes in the threat landscape are assessed on development/engineering practices, tools, and techniques. There shall be a well-documented process for patching and remediating products. There should be a process for informing an acquirer of notification and remediation mechanisms.	SE_MTL.01	Changes to the threat landscape should be monitored by periodically reviewing industry security alerts/bulletins.
Secure Development and Engineering	Monitor and Assess the Impact of Changes in the Threat Landscape		SE_MTL.02	Changes to the development/engineering practices, tools, and techniques shall be assessed in light of changes to the threat landscape.
Secure Development and Engineering	Monitor and Assess the Impact of Changes in the Threat Landscape		SE_MTL.03	The cause of product vulnerabilities shall be evaluated and appropriate changes to the development/engineering practices, tools, and techniques identified to mitigate similar vulnerabilities in the future.

Appendix B: Table of NIST References

Jump back to footnote

The below table contains the NIST references found within, and associated with, the individual controls that were considered as part of this review. All references can be found embedded in the controls identified in Section 3.5 “ICT SCRM Security Controls” in: National Institute for Standards and Technology. (2012). Notional Supply Chain Risk Management Practices for Federal Information Systems. (NIST Interagency Report 7622). Washington DC. [online]. https://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7622.pdf

Reference	Title
NIST Special Publication 800-12	An Introduction to Information Security
NIST Special Publication 800-16	Information Technology Security Training Requirements: a Role- and Performance-Based Model
NIST Special Publication 800-18	Guide for Developing Security Plans for Federal Information Systems
NIST Special Publication 800-23	Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products
NIST Special Publication 800-27	Engineering Principles for Information Technology Security
NIST Special Publication 800-28	Guidelines on Active Content and Mobile Code
NIST Special Publication 800-30	Guide for Conducting Risk Assessments
NIST Special Publication 800-34	Contingency Planning Guide for Federal Information Systems
NIST Special Publication 800-35	Guide to Information Technology Security Services
NIST Special Publication 800-36	Guide to Selecting Information Technology Security Products
NIST Special Publication 800-37	Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
NIST Special Publication 800-39	Managing Information Security Risk: Organization, Mission, and Information System View
NIST Special Publication 800-40	Guide to Enterprise Patch Management Technologies
NIST Special Publication 800-41	Guidelines on Firewalls and Firewall Policy
NIST Special Publication 800-43	System Administration Guidance for Securing Windows 2000
NIST Special Publication 800-46	Guide to Enterprise Telework, Remote Access, and BYOD Security
NIST Special Publication 800-47	Security Guide for Interconnecting Information Systems
NIST Special Publication 800-48	Guide to Securing Legacy IEEE 802.11 Wireless Networks

NIST Special Publication 800-50	Building and Information Technology Security Awareness and Training Program
NIST Special Publication 800-52	Guidelines for the Section, Configuration, and Use of Transport Layer Security (TLS) Implementations
NIST Special Publication 800-53	Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Effective Assessment Plans
NIST Special Publication 800-56	Recommendation for Pair-Wise Key-Establishment Cryptography
NIST Special Publication 800-57	Recommendations for Key-Management
NIST Special Publication 800-60	Guide for Mapping Types of Information and Information Systems to Security Categories
NIST Special Publication 800-61	Computer Security Incident Handling Guide
NIST Special Publication 800-63	Digital Identity Guidelines
NIST Special Publication 800-64	Security Considerations in the System Development Lifecycle
NIST Special Publication 800-65	Integrating IT Security into the Capital Planning and Investment Control Process
NIST Special Publication 800-70	National Checklist Program for IT Products: Guidelines for Checklist Users and Developers
NIST Special Publication 800-73	Interfaces for Personal Identity Verification
NIST Special Publication 800-76	Biometric Specifications for Personal Identity Verification
NIST Special Publication 800-77	Guide to Ipsec VPNs
NIST Special Publication 800-78	Cryptographic Algorithms and Key Sizes for Personal Identity Verification
NIST Special Publication 800-81	Secure Domain Name System (DNS) Development Guide
NIST Special Publication 800-83	Guide to Malware Incident Prevention and Handling for Desktop and Laptops
NIST Special Publication 800-88	Guidelines for Media Sanitization
NIST Special Publication 800-92	Guide to Security Log Management
NIST Special Publication 800-94	Guide to Intrusion Detection and Prevention Systems (IDPS)
NIST Special Publication 800-97	Establishing Wireless Robust Security Networks: A Guide to IEEE
NIST Special Publication 800-100	Information Security Handbook for Managers
NIST Special Publication 800-111	Guide to Storage Encryption Technologies for End User Devices
NIST Special Publication 800-113	Guide to SSL VPNs

NIST Special Publication 800-114	Users Guide to BYOD Security
NIST Special Publication 800-115	Technical Guide to Information Security Testing and Assessment
NIST Special Publication 800-116	Guidelines for the Use of PIV Credentials
NIST Special Publication 800-121	Guide to Bluetooth Security
NIST Special Publication 800-124	Guidelines for Managing the Security of the Mobile Devices in the Enterprise
NIST Special Publication 800-128	Guide for Security-Focused Configuration Management of Information Systems
NIST Special Publication 800-137	Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
NIST Special Publication 800-147	BIOS Protection Guidelines
NIST Special Publication 800-155	BIOS Integrity Measurement Guidelines
NIST Special Publication 800-161	Supply Chain Risk Management Practices for Federal Information Systems and Organizations
NIST Special Publication 800-164	Guidelines for Hardware-Rooted Security in Mobile Devices
NIST Special Publication 800-167	Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
DOD 8551.01	Ports, Protocols, and Services Management
Executive Order 13587	Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information
FICAM Roadmap and Implementation Guidance	FICAM Roadmap and Implementation Guidance
FIPS 140-2	Security Requirements for Cryptographic Modules
FIPS 197	Advanced Encryption Standards
FIPS 199	Standards for Security Categorization of Federal Information and Information Systems
FIPS 200	Minimum Security Requirements for Federal Information and Information Systems
FIPS 201	Personal Identity Verification (PIV) of Federal Employees and Contractors
ISO/IEC 15408	"Protection of Assets from Unauthorized Disclosure, Modification, or Loss of Use."
National Strategy for Trusted Identities in Cyberspace	National Strategy for Trusted Identities in Cyberspace

NIST Interagency Report 7622	Notional Supply Chain Risk Management Practices for Federal Information Systems
OMB A-130	Managing Information as a Strategic Resource
OMB M-02-01	Guidance for Preparing and Submitting Security Plans of Action and Milestones
OMB M-04-04	E-Authentication Guidance for Federal Agencies
OMB M-06-16	Protection of Sensitive Information
OMB M-07-11	Implementation of Commonly Accepted Security Configurations for Windows Operating Systems
OMB M-07-18	Ensuring New Acquisitions Include Common Security Configurations
OMB M-08-22	Guidance on the Federal Desktop Core Configuration (FDCC)
OMB M-11-11	Continued Implementation of Homeland Security Presidential Directive (HSPD) 12- Policy for a Common Identification Standard for Federal Employees and Contractors
OMB M-11-33	FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management

Appendix C: Table of NIST 800-161 Controls

Jump back to footnote

The below table contains the list of the NIST controls that were reviewed, considered, and vetted as part of this review. Source information can be found at: National Institute of Standards and Technology. (2015). Supply Chain Risk Management Practices for Federal Information Systems and Organizations. (NIST SP 800-161). Washington, D.C.: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf

Family	Control Number	Control	Control Enhancement	Org	Mis	Sys
Access Control	AC-1	ACCESS CONTROL POLICY AND PROCEDURES		X	X	X
Access Control	AC-2	ACCOUNT MANAGEMENT			X	X
Access Control	AC-3	ACCESS ENFORCEMENT			X	X
Access Control	AC-4	INFORMATION FLOW ENFORCEMENT			X	X
Access Control	AC-5	SEPARATION OF DUTIES			X	X
Access Control	AC-6	LEAST PRIVILEGE			X	X
Access Control	AC-17	REMOTE ACCESS			X	X
Access Control	AC-18	WIRELESS ACCESS		X	X	X
Access Control	AC-19	ACCESS CONTROL FOR MOBILE DEVICES			X	X
Access Control	AC-20	USE OF EXTERNAL INFORMATION SYSTEMS		X	X	X
Access Control	AC-21	INFORMATION SHARING		X	X	
Access Control	AC-22	PUBLICLY ACCESSIBLE CONTENT			X	X
Access Control	AC-24	ACCESS CONTROL DECISIONS		X	X	X
Awareness and Training	AT-1	SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES		X	X	
Awareness and Training	AT-3	ROLE BASED SECURITY TRAINING				
Audit and Accountability	AU-1	AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES		X	X	X
Audit and Accountability	AU-2	AUDIT EVENTS		X	X	X
Audit and Accountability	AU-6	AUDIT REVIEW, ANALYSIS, AND REPORTING			X	X
Audit and Accountability	AU-10	NON-REPUDIATION				X
Audit and Accountability	AU-12	AUDIT GENERATION			X	X

Audit and Accountability	AU-13	MONITORING FOR INFORMATION DISCLOSURE			X	X
Audit and Accountability	AU-16	CROSS-ORGANIZATIONAL AUDITING			X	X
Security Assessments and Authorizations	CA-1	SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES		X	X	X
Security Assessments and Authorizations	CA-2	SECURITY ASSESSMENTS			X	X
Security Assessments and Authorizations	CA-3	SYSTEM INTERCONNECTIONS				X
Security Assessments and Authorizations	CA-5	PLAN OF ACTION AND MILESTONES			X	X
Security Assessments and Authorizations	CA-6	SECURITY AUTHORIZATION		X	X	X
Security Assessments and Authorizations	CA-7	CONTINUOUS MONITORING		X	X	X
Configuration Management	CM-1	CONFIGURATION MANAGEMENT POLICY AND PROCEDURES		X	X	X
Configuration Management	CM-2	BASELINE CONFIGURATION			X	X
Configuration Management	CM-3	CONFIGURATION CHANGE CONTROL			X	X
Configuration Management	CM-4	SECURITY IMPACT ANALYSIS				X
Configuration Management	CM-5	ACCESS RESTRICTIONS FOR CHANGE			X	X
Configuration Management	CM-6	CONFIGURATION SETTINGS			X	X
Configuration Management	CM-7	LEAST FUNCTIONALITY				X
Configuration Management	CM-8	INFORMATION SYSTEM COMPONENT INVENTORY			X	X
Configuration Management	CM-9	CONFIGURATION MANAGEMENT PLAN			X	X

Configuration Management	CM-10	SOFTWARE USAGE RESTRICTIONS				
Configuration Management	CM-11	USER-INSTALLED SOFTWARE			X	X
Contingency Planning	CP-1	CONTINGENCY PLANNING POLICY AND PROCEDURES		X	X	X
Contingency Planning	CP-2	CONTINGENCY PLAN			X	X
Contingency Planning	CP-6	ALTERNATE STORAGE SITE			X	X
Contingency Planning	CP-7	ALTERNATE PROCESSING SITE			X	X
Contingency Planning	CP-8	TELECOMMUNICATIONS SERVICES			X	X
Identification and Authentication	IA-1	IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES		X	X	X
Identification and Authentication	IA-2	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)		X	X	X
Identification and Authentication	IA-4	IDENTIFIER MANAGEMENT			X	X
Identification and Authentication	IA-5	AUTHENTICATOR MANAGEMENT				X
Identification and Authentication	IA-8	IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)			X	X
Incident Response	IR-1	INCIDENT RESPONSE POLICY AND PROCEDURES		X	X	X
Incident Response	IR-4	INCIDENT HANDLING				
Incident Response	IR-6	INCIDENT REPORTING				
Incident Response	IR-9	INFORMATION SPILLAGE RESPONSE				X
Maintenance	MA-1	SYSTEM MAINTENANCE POLICY AND PROCEDURES		X	X	X
Maintenance	MA-2	CONTROLLED MAINTENANCE				
Maintenance	MA-3	MAINTENANCE TOOLS			X	X
Maintenance	MA-4	NONLOCAL MAINTENANCE			X	X
Maintenance	MA-5	MAINTENANCE PERSONNEL			X	X
Maintenance	MA-6	TIMELY MAINTENANCE				X

Media Protection	MP-1	MEDIA PROTECTION POLICY AND PROCEDURES		X	X	
Media Protection	MP-5	MEDIA TRANSPORT		X	X	
Media Protection	MP-6	MEDIA SANITIZATION			X	X
Physical and Environmental Protection	PE-1	PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES		X	X	X
Physical and Environmental Protection	PE-3	PHYSICAL ACCESS CONTROL			X	X
Physical and Environmental Protection	PE-6	MONITORING PHYSICAL ACCESS				X
Physical and Environmental Protection	PE-16	DELIVERY AND REMOVAL				X
Physical and Environmental Protection	PE-17	ALTERNATE WORK SITE				X
Physical and Environmental Protection	PE-18	LOCATION OF INFORMATION SYSTEM COMPONENTS		X	X	X
Physical and Environmental Protection	PE-20	ASSET MONITORING AND TRACKING			X	X
Planning	PL-1	SECURITY PLANNING POLICY AND PROCEDURES		X		
Planning	PL-2	SYSTEM SECURITY PLAN				X
Planning	PL-8	INFORMATION SECURITY ARCHITECTURE			X	X
Program Management	PM-1	INFORMATION SECURITY PROGRAM PLAN		X	X	X
Program Management	PM-2	SENIOR INFORMATION SECURITY OFFICER		X	X	X
Program Management	PM-3	INFORMATION SECURITY RESOURCES		X	X	X
Program Management	PM-11	MISSION/BUSINESS PROCESS DEFINITION		X	X	X

Program Management	PM-12	INSIDER THREAT PROGRAM		X	X	X
Program Management	PM-16	THREAT AWARENESS PROGRAM		X	X	X
Personnel Security	PS-1	PERSONNEL SECURITY POLICY AND PROCEDURES		X	X	X
Personnel Security	PS-6	ACCESS AGREEMENTS			X	
Personnel Security	PS-7	THIRD-PARTY PERSONNEL SECURITY			X	
Risk Assessment	RA-1	RISK ASSESSMENT POLICY AND PROCEDURES		X	X	X
Risk Assessment	RA-2	SECURITY CATEGORIZATION		X	X	X
Risk Assessment	RA-3	RISK ASSESSMENT		X	X	X
System and Service Acquisition Policy	SA-1	SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES		X	X	X
System and Service Acquisition Policy	SA-2	ALLOCATION OF RESOURCES		X	X	
System and Service Acquisition Policy	SA-3	SYSTEM DEVELOPMENT LIFE CYCLE		X	X	X
System and Service Acquisition Policy	SA-4	ACQUISITION PROCESS		X	X	X
System and Service Acquisition Policy	SA-5	INFORMATION SYSTEM DOCUMENTATION				X
System and Service Acquisition Policy	SA-8	SECURITY ENGINEERING PRINCIPLES		X	X	X
System and Service Acquisition Policy	SA-9	EXTERNAL INFORMATION SYSTEM SERVICES			X	X
System and Service Acquisition Policy	SA-10	DEVELOPER CONFIGURATION MANAGEMENT		X	X	X
System and Service Acquisition Policy	SA-11	DEVELOPER SECURITY TESTING AND EVALUATION		X	X	X
System and Service Acquisition Policy	SA-12	SUPPLY CHAIN PROTECTION		X	X	X
System and Service Acquisition Policy	SA-12 (1)		SUPPLY CHAIN PROTECTION | ACQUISITION STRATEGIES / TOOLS / METHODS		X	X

System and Service Acquisition Policy	SA-12 (2)		SUPPLY CHAIN PROTECTION | SUPPLIER REVIEWS		X	X
System and Service Acquisition Policy	SA-12 (5)		SUPPLY CHAIN PROTECTION | LIMITATION OF HARM		X	X
System and Service Acquisition Policy	SA-12 (7)		SUPPLY CHAIN PROTECTION | ASSESSMENTS PRIOR TO SELECTION / ACCEPTANCE / UPDATE		X	X
System and Service Acquisition Policy	SA-12 (8)		SUPPLY CHAIN PROTECTION | USE OF ALL-SOURCE INTELLIGENCE		X	X
System and Service Acquisition Policy	SA-12 (9)		SUPPLY CHAIN PROTECTION | OPERATIONS SECURITY		X	X
System and Service Acquisition Policy	SA-12 (10)		SUPPLY CHAIN PROTECTION | VALIDATE AS GENUINE AND NOT ALTERED		X	X
System and Service Acquisition Policy	SA-12 (11)		SUPPLY CHAIN PROTECTION | PENETRATION TESTING / ANALYSIS OF ELEMENTS, PROCESSES, AND ACTORS		X	X
System and Service Acquisition Policy	SA-12 (12)		SUPPLY CHAIN PROTECTION | INTER-ORGANIZATIONAL AGREEMENTS		X	X
System and Service Acquisition Policy	SA-12 (13)		SUPPLY CHAIN PROTECTION | CRITICAL INFORMATION SYSTEM COMPONENTS		X	X
System and Service Acquisition Policy	SA-12 (14)		SUPPLY CHAIN PROTECTION | IDENTITY AND TRACEABILITY		X	X
System and Service Acquisition Policy	SA-12 (15)		SUPPLY CHAIN PROTECTION | PROCESSES TO ADDRESS WEAKNESSES OR DEFICIENCIES		X	X
System and Service Acquisition Policy	SA-13	TRUSTWORTHINESS			X	X
System and Service Acquisition Policy	SA-14	CRITICALITY ANALYSIS			X	X

System and Service Acquisition Policy	SA-15	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS			X	X
System and Service Acquisition Policy	SA-16	DEVELOPER-PROVIDED TRAINING			X	X
System and Service Acquisition Policy	SA-17	DEVELOPER SECURITY ARCHITECTURE AND DESIGN		X	X	X
System and Service Acquisition Policy	SA-18	TAMPER RESISTANCE AND DETECTION			X	X
System and Service Acquisition Policy	SA-19	COMPONENT AUTHENTICITY			X	X
System and Service Acquisition Policy	SA-20	CUSTOMIZED DEVELOPMENT OF CRITICAL COMPONENTS			X	X
System and Service Acquisition Policy	SA-21	DEVELOPER SCREENING		X	X	X
System and Service Acquisition Policy	SA-22	UNSUPPORTED SYSTEM COMPONENTS			X	X
System and Communications Protection	SC-1	SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES			X	X
System and Communications Protection	SC-4	INFORMATION IN SHARED RESOURCES			X	X
System and Communications Protection	SC-5	DENIAL OF SERVICE PROTECTION		X	X	X
System and Communications Protection	SC-7	BOUNDARY PROTECTION			X	X
System and Communications Protection	SC-8	TRANSMISSION CONFIDENTIALITY AND INTEGRITY			X	X
System and Communications Protection	SC-18	MOBILE CODE				X

System and Communications Protection	SC-27	PLATFORM-INDEPENDENT APPLICATIONS			X	X
System and Communications Protection	SC-28	PROTECTION OF INFORMATION AT REST			X	X
System and Communications Protection	SC-29	HETEROGENEITY			X	X
System and Communications Protection	SC-30	CONCEALMENT AND MISDIRECTION				X
System and Communications Protection	SC-36	DISTRIBUTED PROCESSING AND STORAGE			X	X
System and Communications Protection	SC-37	OUT-OF-BAND CHANNELS				
System and Communications Protection	SC-38	OPERATIONS SECURITY			X	X
System and Information Protection	SI-1	SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES		X	X	X
System and Information Protection	SI-2	FLAW REMEDIATION			X	X
System and Information Protection	SI-4	INFORMATION SYSTEM MONITORING		X	X	X
System and Information Protection	SI-5	SECURITY ALERTS, ADVISORIES, AND DIRECTIVES			X	X
System and Information Protection	SI-7	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY			X	X
System and Information Protection	SI-12	INFORMATION HANDLING AND RETENTION				X

Appendix D: Table of NIST IR 7622 Supplier Requirements

The below table contains the list of the supplier requirements identified in NIST IR 7622 that were considered as part of this review. Source information can be found at: National Institute for Standards and Technology. (2012). Notional Supply Chain Risk Management Practices for Federal Information Systems. (NIST Interagency Report 7622). Washington DC. [online]. https://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7622.pdf

NIST Supplier Requirements 7622 Notional Supply Chain Risk Management Practices for Federal Information Systems
Uniquely Identify Supply Chain Elements, Processes, and Actors
4.1.3 Suppliers -– General Requirements
a) Apply unique identification requirements to delivered elements (e.g., serial numbers, date codes, license labels, etc.).
b) Ensure that identification methods are sufficient to support provenance in the event of a supply chain issue or adverse supply chain event.
c) Establish policies and procedures that require identification methods to support provenance in the event of a supply chain issue or adverse supply chain event.
d) Define, design, and implement roles that limit privilege and create redundancy throughout the element life cycle to mitigate the risk of a single role being able to, intentionally or unintentionally, create adverse consequences.
e) Require protection and safeguarding of authentication mechanisms.
4.1.5 Suppliers – Technical Implementation Requirements
None
4.1.8 Suppliers – Verification and Validation Requirements
Report deficiencies discovered in critical elements (per acquirer/integrator) up the supply chain for corrective action to ensure that requirements for unique identification are fulfilled.
Limit Access and Exposure within the Supply Chain
4.2.3 Supplier – General Requirements
Use access control mechanisms that limit access to sensitive information.
4.2.5 Supplier – Technical Implementation Requirements

Document the instantiation of audit mechanisms used to audit access control procedures (e.g., audit logs, access reports, and security incident tracking reports).
4.2.8 Supplier – Verification and Validation Requirements
a) Demonstrate use of access control mechanisms across the system or element life cycle and the associated supply chain.
b) Demonstrate ability to intervene in a timely manner to prevent or reduce adverse consequences within the supply chain.
Establish and Maintain the Provenance of Elements, Processes, Tools, and Data
4.3.3 Suppliers – General Requirements
a) Provide evidence of formal processes for documenting roles, responsibilities, and procedures to include the management information and documentation for establishing provenance.
b) Provide evidence on element baselines and maintenance throughout the system or element life cycle, including as part of logistics. Establish and implement a policy to monitor and maintain a valid baseline.
c) Identify and implement appropriate levels of confidentiality, integrity, and availability including spare parts and warehoused systems/elements.
d) Ensure that the provenance of supply chain configuration items (e.g., in the CM system) is protected from unauthorized access and change.
e) Upon request, make available up-to-date product histories that document element changes including retired elements under warranty.
4.3.5 Suppliers – Technical Implementation Requirements
a) Establish configuration baselines for elements. This helps to detect unauthorized tampering/modification during repairs/refurbishing or unauthorized changes to audit policy or mechanisms of audit mechanisms. For example, consider using RF interrogation of ICs and compare those results to results from known trusted ICs.
b) Ensure evidence that identity management and access control provide auditability with respect to use of the CM system by supplier personnel.
4.3.8 Suppliers – Verification and Validation Requirements
a) Demonstrate effective implementation of provenance processes and activities as well as CM mechanisms.
b) Demonstrate the periodic assessment and testing of security measures to protect the provenance process, documentation, and system of records proposed by the security and system engineering communities.
Share Information within Strict Limits
4.4.3 Suppliers - General Requirements

a) Document applicable information-sharing arrangements including:
b) Separately document the instantiation of the techniques, procedures, and tools used to implement information-sharing agreements, and include the identity of participants in information-sharing activities, the means by which information sharing is executed, the mechanisms used to provide protection of information commensurate with the importance of or sensitivity of the information being shared, and the planned and executed audits of information-sharing activities.
c) Document various tactics, techniques, procedures, and tools that could be employed to protect information-sharing mechanisms and processes against unauthorized access or unauthorized use of information included in information-sharing activities and processes.
4.4.5 Suppliers - Technical Implementation Requirements
a) Identify mechanisms, techniques, and procedures that can be used to facilitate the sharing of information and match them with the content, data type, and data volume to be shared so that information sharing:
b) Document technical specifications and measures to protect supply chain processes including element production, assembly, packaging, delivery, testing, and support to understand, evaluate, and minimize opportunities for unauthorized exposure of, or access to, critical elements or processes that could result in loss or compromise of confidentiality, integrity, or availability.
c) Limit disclosure of delivery process information. Limit disclosure of testing methods and procedures, test data, and communication routes by which such data is distributed, analyzed, and reported.
4.4.8 Suppliers - Verification and Validation Requirements
a) Document the assessment and implementation of protection mechanisms regarding information-sharing activities by establishing combinations of information security, IA, physical security, personnel security, and operations security activities.
b) Audit the effectiveness of information-sharing policies and their implementation.
c) Verify and document the implementation of identity management, access controls, and CM to information-sharing activities and the confidentiality, integrity, and availability data and information being included in such activities.
d) Document the processes for sharing information in response to the compromise or loss of confidentiality, integrity, and availability of information, supply chain elements, or supply chain processes.
Perform Supply Chain Risk Management Awareness and Training
4.5.3 Supplier – General Requirements
Provide evidence of the existence of training for appropriate supplier staff on standard commercial practices for acquiring secondary market (refurbished) items, to ensure that secondary market items are adequately supported and maintained.
4.5.5 Supplier – Technical Implementation Requirements

Establish policy and procedures that require receiving personnel (such as technical personnel, equipment specialists, and item managers) to be trained on organizational processes for receiving elements/services (including spare parts), including any known anomalies in parts (which may indicate counterfeits, subversion, or quality issues).
4.5.8 Supplier - Verification and Validation Requirements
a) Demonstrate the implementation and operation of SCRM training and awareness program within the supplier organization.
Use Defensive Design for Systems, Elements, and Processes
4.6.3 Suppliers – General Requirements
a) Document the uses of processes by which elements are selected for use in systems. Specify the use of genuine and tested elements.
b) Report to the acquirer any element maintenance changes, standard interface changes, patches, and upgrades with any associated vulnerabilities. Leverage industry best practice for security patches to include a list of what issues are “covered” in the patches (i.e., the nature of the issues, a severity rating such as CVSS, etc.).
c) Deliver, where appropriate, sufficiently robust elements that do not degrade in performance, even when out-of-bounds inputs are provided (where practicable).
d) If available, provide assessment results of potential failure modes and effects on various proposed element designs based on the application of observed adversary tactics, techniques, procedures, and tools.
e) Establish reviews as a practice (e.g., manual or using automated tools) to be employed as appropriate into the element life cycle, to identify and remediate any weaknesses and vulnerabilities; include peer reviews (e.g., walk-throughs and inspections) and comprehensive or sampled reviews.
f) Establish processes that address code changes that are authorized, validated, and tested (to ensure that they do not introduce regressions or break other functionality).
g) Notify the acquirer and the integrator when counterfeit products are found in the supply chain.
h) Ensure the use of processes that limit entrance of counterfeit items into the supply chain and when entered/breached, the processes for corrective action.
4.6.5 Suppliers – Technical Implementation Requirements
a) Document various defensive design techniques used on the logical and physical design, manufacturing, and supply chain environment.
b) Document the variety of testing techniques used to verify whether the element can be trusted.
c) Provide elements “secured by default” at a level appropriate to the requirements of the acquirer or integrator (e.g., configuration guides).
d) Deliver elements in a manner that facilitates proof of authenticity verification by the acquirer.

e) Verify and document the use of both negative and positive tests to ascertain that the system/element/process does what it is supposed to do and does not do what it should not do.
g) Establish a trusted baseline for the element and operational configuration. Use this baseline to identify unauthorized changes or tampering.
h) Use existing vulnerability and incident management capabilities to identify potential supply chain vulnerabilities.
a) Implement appropriate system and organizational certification requirements to provide rigor in the process to demonstrate a quality assurance mechanism's facet of defensive design. A management system certification, such as ISO 9001, ISO/IEC 27001, or ISO 28000, may provide evidence of quality assurance, security, and supply chain management processes.
from the expected (or baseline) operational profile. Such profiles should consider time of use, information being used (e.g., directories),
4.7.3 Suppliers – General Requirements
None
None
4.7.8 Suppliers – Verification and Validation Requirements
None
Strengthen Delivery Mechanisms
4.8.3 Suppliers - General Requirements
a) Establish a minimum baseline for supply chain delivery, processes, and mechanisms. Where appropriate, use trusted contacts and ship via a protected carrier (such as U.S. registered mail, using cleared/official couriers, or a diplomatic pouch). Protect the system and element while storing before use (including spares).
b) Implement delivery processes for the intended logical and physical transfer and receipt of elements to be done by authorized personnel.

c) Provide documentation of any nondestructive techniques or mechanisms to determine if there is any unauthorized access throughout the delivery process.
4.8.5 Suppliers - Technical Implementation Requirements
a) Use and check difficult-to-forge marks (such as digital signatures or hologram, DNA, and nano tags) for all critical elements.
b) Document any anti-tamper mechanisms used for prevention and discovery, including tamper-resistant and tamper-evident packaging (e.g., tamper tape or seals). These must be difficult to remove or replace undetected.
c) Document and monitor the logical delivery of elements, requiring downloading from approved, verification-enhanced sites. Consider encrypting elements (software, software patches, etc.) at rest and in motion throughout delivery. For mechanisms that use cryptographic algorithms, consider compliance with NIST FIPS 140-2.
d) Document and resolve potential attacks on delivery mechanisms to estimate and evaluate potential loss or compromise of confidentiality, integrity, or availability of elements.
e) Obtain chain of custody for all critical hardware and require tamper-evident packaging.
4.8.8 Suppliers - Verification and Validation Requirements
None
Assure Sustainment Activities and Processes
4.9.3 Suppliers – General Requirements
None
4.9.5 Supplier – Technical Implementation Requirements
None
4.9.8 Supplier – Verification and Validation Activities
None
Manage Disposal and Final Disposition Activities throughout the System or Element Life Cycle
4.10.3 Suppliers - General Requirements
a) Establish relationships with trusted disposers who have documented an effective disposal process.
b) Implement processes and procedures for the secure and permanent destruction of elements, as appropriate.

4.10.5 Suppliers - Technical Implementation Requirements
a) Manage and properly dispose of all scrap materials, out-of-specification elements, or suspected or confirmed defective, counterfeit, or tampered elements.
b) Establish processes used to identify all elements/sub-elements that need to be specially disposed of (including HAZMAT/explosive ordinance/environment impact, confidential equipment, etc.).
c) Document the process used to carefully move or save data so that it does not harm, lose, or corrupt required information and does not
d) Describe technical limitations related to disposal activities (e.g., degaussed media cannot be reused and will void warranties).
4.10.8 Suppliers - Verification and Validation Requirements
a) Regularly review the disposal process.
b) Verify and validate the identification and tracking of items subject to preservation for forensics and evidentiary purposes and/or controlled disposal.

Appendix E: Table of Proposed Controls in NIST 800-161rev.1

Jump back to footnote

The below table contains the list of the controls in the public comment release of NIST 800-161.rev.1 that were considered as part of this review. Controls that were added or changed are indicated in gray. Controls that were eliminated are indicated with a strikethrough. The public comment period pertaining to these draft standards closes on June 14, 2021. Source information can be found at: National Institute for Standards and Technology. (2021). Cyber Supply Chain Risk Management Practices for System and Organizations. (NIST SP 800-161.rev.1). Washington DC. [online]. https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/draft

Family	Control Number	Control
Access Control	AC-1	ACCESS CONTROL POLICY AND PROCEDURES
Access Control	AC-2	ACCOUNT MANAGEMENT
Access Control	AC-3	ACCESS ENFORCEMENT
Access Control	AC-4	INFORMATION FLOW ENFORCEMENT
Access Control	AC-5	SEPARATION OF DUTIES
Access Control	AC-6	LEAST PRIVILEGE
Access Control	AC-17	REMOTE ACCESS
Access Control	AC-18	WIRELESS ACCESS
Access Control	AC-19	ACCESS CONTROL FOR MOBILE DEVICES
Access Control	AC-20	USE OF EXTERNAL INFORMATION SYSTEMS
Access Control	AC-21	INFORMATION SHARING
Access Control	AC-22	PUBLICLY ACCESSIBLE CONTENT
Access Control	**AC-23**	**DATA MINING PROTECTION**
Access Control	AC-24	ACCESS CONTROL DECISIONS
Awareness and Training	AT-1	SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES
Awareness and Training	**AT-2**	**LITERACY TRAINING AND AWARENESS**
Awareness and Training	AT-3	ROLE BASED SECURITY TRAINING
Awareness and Training	**AT-4**	**TRAINING RECORDS**
Audit and Accountability	AU-1	AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES
Audit and Accountability	AU-2	**EVENT LOGGING**
Audit and Accountability	**AU-3**	**CONTENT OF AUDIT RECORDS**

Audit and Accountability	AU-6	AUDIT REVIEW, ANALYSIS, AND REPORTING
Audit and Accountability	AU-10	NON-REPUDIATION
Audit and Accountability	AU-12	**AUDIT RECORD GENERATION**
Audit and Accountability	AU-13	MONITORING FOR INFORMATION DISCLOSURE
Audit and Accountability	**AU-14**	**SESSION AUDIT**
Audit and Accountability	AU-16	CROSS-ORGANIZATIONAL AUDITING
Assessment, Authorization, and Monitoring	CA-1	POLICY AND PROCEDURES
Assessment, Authorization, and Monitoring	CA-2	CONTROL ASSESSMENTS
Assessment, Authorization, and Monitoring	CA-3	INFORMATION EXCHANGE
Assessment, Authorization, and Monitoring	CA-5	PLAN OF ACTION AND MILESTONES
Assessment, Authorization, and Monitoring	CA-6	AUTHORIZATION
Assessment, Authorization, and Monitoring	CA-7	CONTINUOUS MONITORING
Configuration Management	CM-1	POLICY AND PROCEDURES
Configuration Management	CM-2	BASELINE CONFIGURATION
Configuration Management	CM-3	CONFIGURATION CHANGE CONTROL
Configuration Management	CM-4	IMPACT ANALYSIS
Configuration Management	CM-5	ACCESS RESTRICTIONS FOR CHANGE
Configuration Management	CM-6	CONFIGURATION SETTINGS
Configuration Management	CM-7	LEAST FUNCTIONALITY
Configuration Management	CM-8	SYSTEM COMPONENT INVENTORY
Configuration Management	CM-9	CONFIGURATION MANAGEMENT PLAN
Configuration Management	CM-10	SOFTWARE USAGE RESTRICTIONS
Configuration Management	CM-11	USER-INSTALLED SOFTWARE
Configuration Management	CM-12	INFORMATION LOCATION
Configuration Management	**CM-13**	**DATA ACTION MAPPING**
Configuration Management	**CM-14**	**SIGNED COMPONENTS**
Contingency Planning	CP-1	POLICY AND PROCEDURES
Contingency Planning	CP-2	CONTINGENCY PLAN
Contingency Planning	**CP-3**	**CONTINGENCY TRAINING**
Contingency Planning	**CP-4**	**CONTINGENCY PLAN TESTING**

Contingency Planning	CP-6	ALTERNATE STORAGE SITE
Contingency Planning	CP-7	ALTERNATE PROCESSING SITE
Contingency Planning	CP-8	TELECOMMUNICATIONS SERVICES
Contingency Planning	**CP-11**	**ALTERNATE COMMUNICATIONS PROTOCOLS**
Identification and Authentication	IA-1	POLICY AND PROCEDURES
Identification and Authentication	IA-2	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)
Identification and Authentication	**IA-3**	**DEVICE IDENTIFICATION AND AUTHENTICATION**
Identification and Authentication	IA-4	IDENTIFIER MANAGEMENT
Identification and Authentication	IA-5	AUTHENTICATOR MANAGEMENT
Identification and Authentication	IA-8	IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)
Identification and Authentication	**IA-9**	**SERVICE IDENTIFICATION AND AUTHENTICATION**
Incident Response	IR-1	POLICY AND PROCEDURES
Incident Response	**IR-2**	**INCIDENT RESPONSE TRAINING**
Incident Response	**IR-3**	**INCIDENT RESPONSE TESTING**
Incident Response	IR-4	INCIDENT HANDLING
Incident Response	**IR-5**	**INCIDENT MONITORING**
Incident Response	IR-6	INCIDENT REPORTING
Incident Response	**IR-7**	**INCIDENT RESPONSE ASSISTANCE**
Incident Response	**IR-8**	**INCIDENT RESPONSE PLAN**
Incident Response	IR-9	INFORMATION SPILLAGE RESPONSE
Maintenance	MA-1	POLICY AND PROCEDURES
Maintenance	MA-2	CONTROLLED MAINTENANCE
Maintenance	MA-3	MAINTENANCE TOOLS
Maintenance	MA-4	NONLOCAL MAINTENANCE
Maintenance	MA-5	MAINTENANCE PERSONNEL
Maintenance	MA-6	TIMELY MAINTENANCE
Maintenance	**MA-7**	**FIELD MAINTENANCE**
Maintenance	**MA-8**	**MAINTENANCE MONITORING AND INFORMATION SHARING (NEW)**
Media Protection	MP-1	POLICY AND PROCEDURES
Media Protection	**MP-4**	**MEDIA STORAGE**

Media Protection	MP-5	MEDIA TRANSPORT
Media Protection	MP-6	MEDIA SANITIZATION
Physical and Environmental Protection	PE-1	POLICY AND PROCEDURES
Physical and Environmental Protection	**PE-2**	**PHYSICAL ACCESS AUTHORIZATIONS**
Physical and Environmental Protection	PE-3	PHYSICAL ACCESS CONTROL
Physical and Environmental Protection	PE-6	MONITORING PHYSICAL ACCESS
Physical and Environmental Protection	PE-16	DELIVERY AND REMOVAL
Physical and Environmental Protection	PE-17	ALTERNATE WORK SITE
Physical and Environmental Protection	PE-18	LOCATION OF INFORMATION SYSTEM COMPONENTS
Physical and Environmental Protection	PE-20	ASSET MONITORING AND TRACKING
Physical and Environmental Protection	**PE-23**	**FACILITY LOCATION**
Planning	PL-1	POLICY AND PROCEDURES
Planning	PL-2	SYSTEM SECURITY AND PRIVACY PLANS
Planning	**PL-4**	**RULES OF BEHAVIOR**
Planning	**PL-5**	**CONCEPT OF OPERATIONS**
Planning	PL-8	INFORMATION SECURITY ARCHITECTURE
Planning	**PL-9**	**CENTRAL MANAGEMENT**
Planning	**PL-10**	**BASELINE SELECTION**
Program Management	PM-1	INFORMATION SECURITY PROGRAM PLAN
Program Management	PM-2	SENIOR INFORMATION SECURITY OFFICER
Program Management	PM-3	INFORMATION SECURITY RESOURCES
Program Management	**PM-4**	**PLAN OF ACTION AND MILESTONES PROCESS**
Program Management	**PM-5**	**SYSTEM INVENTORY**
Program Management	**PM-6**	**MEASURES OF PERFORMANCE**
Program Management	**PM-7**	**ENTERPRISE ARCHITECTURE**
Program Management	**PM-8**	**CRITICAL INFRASTRUCTURE PLAN**
Program Management	**PM-9**	**RISK MANAGEMENT STRATEGY**
Program Management	**PM-10**	**AUTHORIZATION PROCESS**
Program Management	PM-11	MISSION/BUSINESS PROCESS DEFINITION
Program Management	PM-12	INSIDER THREAT PROGRAM

Program Management	**PM-13**	**SECURITY AND PRIVACY WORKFORCE**
Program Management	**PM-14**	**TESTING, TRAINING, AND MONITORING**
Program Management	**PM-15**	**SECURITY AND PRIVACY GROUPS AND ASSOCIATIONS**
Program Management	PM-16	THREAT AWARENESS PROGRAM
Program Management	**PM-17**	**PROTECTING CONTROLLED UNCLASSIFIED INFORMATION ON EXTERNAL SYSTEMS**
Program Management	**PM-18**	**PRIVACY PROGRAM PLAN**
Program Management	**PM-19**	**PRIVACY PROGRAM LEADERSHIP ROLE**
Program Management	**PM-20**	**DISSEMINATION OF PRIVACY PROGRAM INFORMATION**
Program Management	**PM-21**	**ACCOUNTING OF DISCLOSURES**
Program Management	**PM-22**	**PERSONALLY IDENTIFIABLE INFORMATION QUALITY MANAGEMENT**
Program Management	**PM-23**	**DATA GOVERNANCE BODY**
Program Management	**PM-25**	**MINIMIZATION OF PERSONALLY IDENTIFIABLE INFORMATION USED IN TESTING, 4416 TRAINING, AND RESEARCH**
Program Management	**PM-26**	**COMPLAINT MANAGEMENT**
Program Management	**PM-27**	**PRIVACY REPORTING**
Program Management	**PM-28**	**RISK FRAMING**
Program Management	**PM-29**	**RISK MANAGEMENT PROGRAM LEADERSHIP ROLES**
Program Management	**PM-30**	**SUPPLY CHAIN RISK MANAGEMENT STRATEGY**
Program Management	**PM-31**	**CONTINUOUS MONITORING STRATEGY**
Program Management	**PM-32**	**PURPOSING**
Personnel Security	PS-1	POLICY AND PROCEDURES
Personnel Security	**PS-3**	**PERSONNEL SCREENING**
Personnel Security	PS-6	ACCESS AGREEMENTS
Personnel Security	PS-7	EXTERNAL PERSONNEL SECURITY
Personally Identifiable Information P**rocessing and Transparency**	**PT-1**	**POLICY AND PROCEDURES**
Risk Assessment	RA-1	POLICY AND PROCEDURES
Risk Assessment	RA-2	SECURITY CATEGORIZATION
Risk Assessment	RA-3	RISK ASSESSMENT
Risk Assessment	**RA-5**	**VULNERABILITY MONITORING AND SCANNING**

Risk Assessment	**RA-7**	**RISK RESPONSE**
Risk Assessment	**RA-9**	**CRITICALITY ANALYSIS**
Risk Assessment	**RA-10**	**THREAT HUNTING**
System and Service Acquisition Policy	SA-1	POLICY AND PROCEDURES
System and Service Acquisition Policy	SA-2	ALLOCATION OF RESOURCES
System and Service Acquisition Policy	SA-3	SYSTEM DEVELOPMENT LIFE CYCLE
System and Service Acquisition Policy	SA-4	ACQUISITION PROCESS
System and Service Acquisition Policy	SA-5	SYSTEM DOCUMENTATION
System and Service Acquisition Policy	SA-8	SECURITY AND PRIVACY ENGINEERING PRINCIPLES
System and Service Acquisition Policy	SA-9	EXTERNAL INFORMATION SYSTEM SERVICES
System and Service Acquisition Policy	SA-10	DEVELOPER CONFIGURATION MANAGEMENT
System and Service Acquisition Policy	SA-11	DEVELOPER TESTING AND EVALUATION
System and Service Acquisition Policy	SA-12	SUPPLY CHAIN PROTECTION
~~**System and Service Acquisition Policy**~~	~~SA-12 (1)~~	~~SUPPLY CHAIN PROTECTION | ACQUISITION STRATEGIES / TOOLS / METHODS~~
~~**System and Service Acquisition Policy**~~	~~SA-12 (2)~~	~~SUPPLY CHAIN PROTECTION | SUPPLIER REVIEWS~~
~~**System and Service Acquisition Policy**~~	~~SA-12 (5)~~	~~SUPPLY CHAIN PROTECTION | LIMITATION OF HARM~~
~~**System and Service Acquisition Policy**~~	~~SA-12 (7)~~	~~SUPPLY CHAIN PROTECTION | ASSESSMENTS PRIOR TO SELECTION / ACCEPTANCE / UPDATE~~
~~**System and Service Acquisition Policy**~~	~~SA-12 (8)~~	~~SUPPLY CHAIN PROTECTION | USE OF ALL-SOURCE INTELLIGENCE~~
~~**System and Service Acquisition Policy**~~	~~SA-12 (9)~~	~~SUPPLY CHAIN PROTECTION | OPERATIONS SECURITY~~
~~**System and Service Acquisition Policy**~~	~~SA-12 (10)~~	~~SUPPLY CHAIN PROTECTION | VALIDATE AS GENUINE AND NOT ALTERED~~
~~**System and Service Acquisition Policy**~~	~~SA-12 (11)~~	~~SUPPLY CHAIN PROTECTION | PENETRATION TESTING / ANALYSIS OF ELEMENTS, PROCESSES, AND ACTORS~~
~~**System and Service Acquisition Policy**~~	~~SA-12 (12)~~	~~SUPPLY CHAIN PROTECTION | INTER-ORGANIZATIONAL AGREEMENTS~~

~~**System and Service Acquisition Policy**~~	~~SA-12 (13)~~	~~SUPPLY CHAIN PROTECTION | CRITICAL INFORMATION SYSTEM COMPONENTS~~
~~**System and Service Acquisition Policy**~~	~~SA-12 (14)~~	~~SUPPLY CHAIN PROTECTION | IDENTITY AND TRACEABILITY~~
~~**System and Service Acquisition Policy**~~	~~SA-12 (15)~~	~~SUPPLY CHAIN PROTECTION | PROCESSES TO ADDRESS WEAKNESSES OR DEFICIENCIES~~
System and Service Acquisition Policy	SA-13	TRUSTWORTHINESS
System and Service Acquisition Policy	SA-14	CRITICALITY ANALYSIS
System and Service Acquisition Policy	SA-15	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS
System and Service Acquisition Policy	SA-16	DEVELOPER-PROVIDED TRAINING
System and Service Acquisition Policy	SA-17	DEVELOPER SECURITY ARCHITECTURE AND DESIGN
System and Service Acquisition Policy	SA-18	TAMPER RESISTANCE AND DETECTION
System and Service Acquisition Policy	SA-19	COMPONENT AUTHENTICITY
System and Service Acquisition Policy	SA-20	CUSTOMIZED DEVELOPMENT OF CRITICAL COMPONENTS
System and Service Acquisition Policy	SA-21	DEVELOPER SCREENING
System and Service Acquisition Policy	SA-22	UNSUPPORTED SYSTEM COMPONENTS
System and Communications Protection	SC-1	PROTECTION POLICY AND PROCEDURES
System and Communications Protection	SC-4	INFORMATION IN SHARED RESOURCES
System and Communications Protection	SC-5	DENIAL OF SERVICE PROTECTION
System and Communications Protection	SC-7	BOUNDARY PROTECTION
System and Communications Protection	SC-8	TRANSMISSION CONFIDENTIALITY AND INTEGRITY
System and Communications Protection	SC-18	MOBILE CODE
System and Communications Protection	SC-27	PLATFORM-INDEPENDENT APPLICATIONS
System and Communications Protection	SC-28	PROTECTION OF INFORMATION AT REST
System and Communications Protection	SC-29	HETEROGENEITY
System and Communications Protection	SC-30	CONCEALMENT AND MISDIRECTION
System and Communications Protection	SC-36	DISTRIBUTED PROCESSING AND STORAGE
System and Communications Protection	SC-37	OUT-OF-BAND CHANNELS
System and Communications Protection	SC-38	OPERATIONS SECURITY
System and Communications Protection	**SC-47**	**ALTERNATE COMMUNICATIONS PATHS**

System and Information Protection	SI-1	POLICY AND PROCEDURES
System and Information Protection	SI-2	FLAW REMEDIATION
System and Information Protection	**SI-3**	**MALICIOUS CODE PROTECTION**
System and Information Protection	SI-4	SYSTEM MONITORING
System and Information Protection	SI-5	SECURITY ALERTS, ADVISORIES, AND DIRECTIVES
System and Information Protection	SI-7	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY
System and Information Protection	SI-12	INFORMATION MANAGEMENT AND RETENTION
System and Information Protection	**SI-20**	**TAINTING**