Software Security in Supply Chains

Introduction

Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*, was released on May 12, 2021, and acknowledges the increasing number of software security risks throughout the supply chain. Federal departments and agencies become exposed to cybersecurity risks through the software and services that they acquire, deploy, use, and manage from their supply chain, which includes open-source software components. Acquired software may contain known and unknown vulnerabilities as a result of the product architecture and development life cycle.

Mitigating these types of risks throughout the supply chain is a cornerstone goal of the EO, with Sections 4(b), 4(c), and 4(d) focusing exclusively on the critical sub-discipline of Cybersecurity Supply Chain Risk Management (C-SCRM) from the lens of federal acquirers:

EO Section 4 Text
(b) Within 30 days of the date of this order, the Secretary of Commerce acting through the Director of NIST shall solicit input from the Federal Government, private sector, academia, and other appropriate actors to **identify existing or develop new standards, tools, and best practices** for complying with the standards, procedures, or criteria in subsection (e) of this section. The guidelines shall include **criteria that can be used to evaluate software security, include criteria to evaluate the security practices of the developers and suppliers themselves**, and identify innovative tools or methods to demonstrate conformance with secure practices.

Relevant directives to this guidance:

(c) Within 180 days of the date of this order, the Director of NIST shall publish **preliminary guidelines, based on the consultations described in subsection (b) of this section and drawing on existing documents as practicable, for enhancing software supply chain security and meeting the requirements of this section.**

(d) Within 360 days of the date of this order, the Director of NIST shall publish additional guidelines that include procedures for periodic review and updating of the guidelines described in subsection (c) of this section.

This guidance is NIST's response to the directives in Section 4(c) and 4(d) of EO 14028.

Existing industry standards, tools, and recommended[1] practices are sourced from:

- NIST's foundational C-SCRM guidance;
- Position papers submitted in advance of NIST's June 2021 Enhancing Software Supply Chain Security Workshop, federal software supply chain security working groups, and an array of public and private industry partnerships; and
- NIST's EO webpage.

To support the prioritization and practical implementation of evolving software supply chain security recommendations, guidance is presented in the *Foundational*, *Sustaining*, and *Enhancing* practices paradigm in SP 800-161r1.

Existing Standards, Tools, and Recommended Practices

Existing industry standards, tools, and recommended practices are sourced from SP 800-161r1upd1, and other NIST guidance published in response to EO 14028. Those initiatives, as outlined by NIST on its EO 14028 guidance webpage, encompass:

- Critical Software Definition
- Security Measures for "EO-Critical Software" Use
- Software Supply Chain Security Guidance
- Recommended Minimum Standards for Vendor or Developer Verification of Software

Guidance in this Appendix does not introduce net new controls but rather frames existing controls for acquirers within the context of EO 14028.

Key Takeaways

- **Using this guidance.** Federal agency acquirers should utilize this guidance to contextualize their application of any existing SP 800-161r1 controls upon their suppliers and — where feasible — adopt new software supply chain security recommendations that previously fell outside of the explicit scope of SP 800-161r1 in the context of EO 14028.
- **Existing standards, tools, and recommended practices.** This guidance provides direction to federal agency acquirers on how to augment existing SP 800-161r1 controls in accordance with EO 14028. It focuses on 1) EO-critical software, 2) software cybersecurity for producers and users, 3) software

[1] NIST interprets the intent of "best" practices within the context of the EO as "recommended" practices to align with its typical mandate as an authoritative body that provides recommendations to both public and private organizations.

verification, and 4) cybersecurity labeling for Internet of Things (IoT) devices and software. This publication complements related workstreams by NIST, NTIA, NSA, DOD, CISA, and OMB.

- **Evolving standards, tools, and recommended practices.** This publication offers recommended software supply chain concepts and capabilities that include a Software Bill of Materials (SBOM), enhanced vendor risk assessments, open-source software controls, and vulnerability management practices. Organizations should prioritize, tailor, and implement these practices and capabilities by applying the Foundational, Sustaining, and Enhancing practices paradigm of SP 800-161r1.

Guidance, Purpose, Scope, and Audience

This guidance informs the acquisition, use, and maintenance of third-party software and services for agencies' information technology (IT), Cybersecurity Supply Chain Risk Management (C-SCRM) Program Management Office, acquisition/procurement, and other functions in response to Section 4(c) and 4(d) of EO 14028. It calls for applying the controls in SP 800-161r1upd1 to suppliers and — where feasible — adopting new software supply chain security recommendations.

The impact of Section 4(c) and 4(d) directives will continue to evolve through 2022 and beyond. The concepts introduced here will similarly evolve. NIST will maintain this guidance in accordance with Section 4(d).

This guidance does not include contractual language for federal agencies or cybersecurity concepts and disciplines beyond core software supply chain security use cases.

The primary audience for this guidance are federal agencies that acquire, deploy, use, and manage software from open-source projects, third-party suppliers, developers, system integrators, external system service providers, and other information and communications technology (ICT)/operational technology (OT)-related service providers that must comply with Section 4(d) of EO 14028. As outlined in Fig. 1, Section 4(e) and the associated SP 800-218 contain guidance on secure software produced or developed in-house by federal agencies or by third-party suppliers.

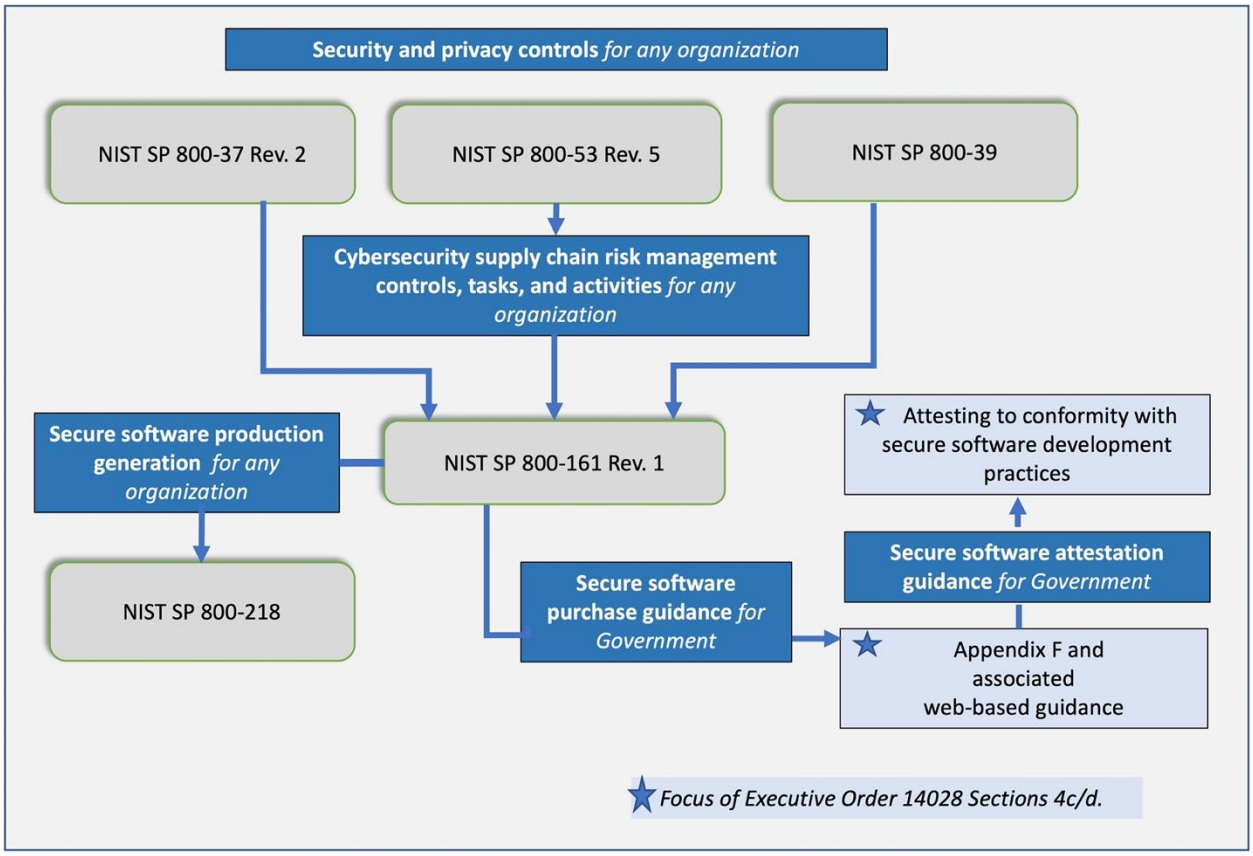

Fig. 1. Relationship map between SSDF V1.1 and EO 14028, Section 4(d)

EO-Critical Software and Security Measures

Following the EO's directive, NIST's definition for critical software reflects "the level of privilege or access required to function" and "integration and dependencies with other software."[2]

NIST has also published guidance outlining the security measures to protect the revised set of designated critical software.

EO-Critical Software Definition

NIST's publication on the definition of critical software enhances traditional notions of context-based criticality with function-based definitions. Table 1 identifies the points at which criticality considerations in SP 800-161r1 may be informed but should not be superseded by the new EO-critical software definition.

Table 1. Impacts of EO-critical software definition on SP 800-161r1 guidance for federal agencies

Section Identifier	Section Title	EO-Critical Definition Impact
2	**Integration of C-SCRM into Enterprise-wide Risk Management**	• Enhance SP 800-39's Assess risk step with EO-critical risk definitions when considering software supply chain components and suppliers.
2.3	**Multilevel Risk Management**	• Augment C-SCRM Strategy and Implementation Plans and Policies. C-SCRM Plans focus on mission- and business-critical requirements to include EO-critical software supply chain security considerations, where applicable.
3.1	**C-SCRM in Acquisition**	• Ensure that groupings accommodate EO-critical suppliers when segmenting the organization's supplier relationships and contracts. • Codify function-based software criticality definitions during the plan procurement step, and incorporate EO-critical concepts when justifying the level of criticality.
3.4	**C-SCRM Key Practices**	• Integrate context-based criticality concepts within the Foundational Practices' measurement

[2] National Institute of Standards and Technology. (2021). Definition of Critical Software Under Executive Order (EO) 14028.

Section Identifier	Section Title	EO-Critical Definition Impact
		of supplier criticality and the utilization of supplier risk assessments. • Expand Sustaining Practices attestation activities to all net new critical suppliers under the expanded EO criticality definition (e.g., suppliers who develop a software component that performs a function critical to trust, regardless of where that component is used within the organization).
Appendix A	**C-SCRM Security Controls**	• Extend EO-critical definition considerations to ICT/OT-related service providers, where applicable.
Appendix C	**Risk Exposure Framework**	• Incorporate EO-critical definition components when determining the organization's acceptable level of risk, particularly within the context of system criticality assessments.
Appendix D	**C-SCRM Templates**	• Account for EO-critical definitions when considering the automated generation of C-SCRM plan elements, such as supply chain component criticality.
Appendix E	**FASCSA**	• Account for risk factors associated with EO-critical definitions when identifying, assessing, and responding to supply chain risks.
Appendix G	**C-SCRM Activities in the Risk Management Process**	• Incorporate EO-critical component definitions when performing risk management activities that include a reference to criticality as part of (i) framing risk, (ii) assessing risk, (iii) responding to risk once determined, and (iv) monitoring risk (i.e., FARM process).

Security Measures (SM) for EO-Critical Software Use

NIST published "Security Measures for 'EO-Critical Software' Use Under EO 14028" in July 2021. Software supply chain security measures are essential for internal decision-making and supplier oversight. Federal agencies must recognize their roles as critical players in the software supply chain and should, at a minimum, internally implement the same security controls that they require of their software suppliers. All of the EO Security Measures should be considered for all software, not just for EO-Critical Software.

Table 2 outlines the mappings and coverage of the EO's security measures across SP 800-161r1 controls, control enhancements, and supplemental guidance. Many of these

are included in the C-SCRM controls baseline.

EO Security Measures and their associated SP 800-161r1 controls (with the exception of AC-6, CA-7, and SR-8) are considered "flow down." Enterprises should require prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors where feasible.

Federal agencies that align with SP 800-161r1 controls should use Table 2 to aid in conforming with EO Security Measures and to ensure their effective application across the software supply chain and acquisition life cycle.

Table 2. C-SCRM controls and security measures crosswalk

Control Identifier	Control Name	C-SCRM Baseline	EO Security Measure
AC-2	**Account Management**	X	1.1, 1.2, 1.3, 2.2
AC-3	**Access Enforcement**	X	2.2
AC-4	**Information Flow Enforcement**		2.4
AC-5	**Separation of Duties**		3.3
AC-6	**Least Privilege**[2]	x[3]	2.2, 3.3
AC-17	**Remote Access**	X	2.4
AT-2	**Literacy Training and Awareness**[2]	X[3]	5.1
AT-3	**Role-based Training**	X	4.5, 5.1, 5.2, 5.3
AU-2	**Event Logging**	X	4.1
AU-3	**Content of Audit Records**	X	4.1
AU-12	**Audit Record Generation**	X	4.1
AU-13	**Monitoring for Information Disclosure**		4.4
AU-14	**Session Audit**		4.4
CA-7	**Continuous Monitoring**[2]	X[3]	3.2, 3.3, 4.1
CM-2	**Baseline Configuration**	X	3.3
CM-3	**Configuration Change Control**		3.3
CM-6	**Configuration Settings**	X	3.3
CM-7	**Least Functionality**	X	3.3
CM-8	**System Component Inventory**	X	2.1, 3.1
CP-3	**Contingency Training**	X	5.2
IA-2	**Identification and Authentication (Organizational Users)**	X	1.1, 1.2
IA-4	**Identifier Management**	X	1.1
IA-5	**Authenticator Management**	X	1.1

[3] While the base control is not addressed in SP 800-161r1, the topic at large is addressed through supplemental guidance provided for control enhancements to the base control.

Control Identifier	Control Name	C-SCRM Baseline	EO Security Measure
IA-9	**Service Identification and Authentication**		1.2
IR-2	**Incident Response Training**	X	4.5
PM-5	**System Inventory**		2.1, 3.1
RA-5	**Vulnerability Monitoring and Scanning**	X	3.2, 3.3
RA-9	**Criticality Analysis**		3.1
SC-7	**Boundary Protection**	X	1.4, 4.4
SC-8	**Transmission Confidentiality and Integrity**		2.4
SC-28	**Protection of Information at Rest**		2.3
SI-2	**Flaw Remediation**	X	3.2
SI-3	**Malicious Code Protection**	X	4.3, 4.4
SI-4	**System Monitoring**	X	4.2, 4.3
SI-5	**Security Alerts, Advisories, and Directives**	X	3.2, 3.3, 4.3
SI-7	**Software, Firmware, and Information Integrity**		4.3
SR-8	**Notification Agreements**	X	3.2

The measures are intended to secure the use of deployed EO-critical software in the operational environments of federal agencies. Security measures for EO-critical software are not intended to be comprehensive, nor do they eliminate the need for other security measures.

One provision in "Security Measures for 'EO-Critical Software' Use Under EO 14028" falls outside of the scope of SP 800-161r1. Security Measure 2.5 outlines a requirement to "back up data, exercise backup restoration, and be prepared to recover data used by EO-critical software and EO-critical software platforms at any time from backups" [3].[4] Though relevant to sound C-SCRM practices, controls related to Security Measure 2.5 are not included in SP 800-161r1 because they are not third-party risk-related. Rather, they focus on managing the software within a system.

Mappings to Security Measure 2.5 and partial security measure mappings outside of the scope of this document are outlined in Table 3. Federal agencies that seek to fully conform with all mapped controls across all EO security measures, regardless of whether they are C-SCRM-specific in nature, may use this table to accelerate conformance or refer directly to "Security Measures for 'EO-Critical Software' Use Under EO 14028."

[4] National Institute of Standards and Technology. (2021). Security Measures for "EO-Critical Software" Use Under Executive Order (EO) 14028.

Table 3. C-SCRM Control and Security Measure Crosswalk

Control Identifier	Control (or Control Enhancement) Name	C-SCRM Baseline	EO Security Measure
AU-4	**Audit Log Storage Capacity**	N/A	4.1
AU-5	**Response to Audit Logging Process Failures**	N/A	4.1
AU-8	**Timestamps**	N/A	4.1
AU-11	**Audit Record Retention**	N/A	4.1
CA-7	**Continuous Monitoring**	N/A	3.2, 3.3, 4.1
CP-9	**System Backup**	N/A	2.5
CP-10	**System Recovery and Reconstitution**	N/A	2.5
SC-2	**Separation of System and User Functionality**	N/A	1.3
SC-7(15)	**Boundary Protection | Networked Privileged Accesses**	N/A	1.3

Software Cybersecurity for Producers and Users

Section 4(e) of EO 14028 outlines 10 actions and outcomes to further secure software development. Since most subsections in this Appendix are specific to software producers and users, federal agencies that seek to implement those actions and achieve those outcomes should refer to SP 800-218 (see below).

A notable exception in NIST's response to 4(e) is its Attesting to Conformity with Secure Software Development Practices, which outlines minimum recommendations for agency purchasers to require attestations from software suppliers.

This guidance considers both SSDF V1.1 and Attesting to Conformity with Secure Software Development Practices within the context of existing C-SCRM standards, tools, and recommended practices for federal agency acquirers, as mandated in Sections 4(c) and 4(d) of EO 14028.

Secure Software Development Framework (SSDF) Version 1.1

SSDF V1.1's core set of high-level secure software development practices are fundamental for software producers and developers. They are also critical for federal agency acquirers who seek to use a common vocabulary with suppliers during acquisition and to augment their existing C-SCRM controls. Table 4 identifies likely areas of impact across supply chain acquisition and procurement activities.

Table 4. C-SCRM controls and SSDF V1.1 crosswalk

Control Identifier	Control (or Control Enhancement) Name	C-SCRM Baseline	SSDF V1.1 Task(s)
SA-1	**Policy and Procedures**	x	PO.1.1
SA-3	**System Development Life Cycle**	x	PO.2.1, PO.5.1
SA-4	**Acquisition Process**	x	PO.1.3, PW.4.1, PW.4.4
SA-5	**System Documentation**	x	PW.4.1, PW.9.2, RV.2.2
SA-8	**Security and Privacy Engineering Principles**	x	PO.1.1, PO.1.2, PO.2.2, PO.5.1, PS.1.1, PS.2.1, PS.3.1, PS.3.2, PW.1.1, PW.1.2, PW.4.4, RV.2.2
SA-9(1)	**External System Services | Risk Assessments and Organizational Approvals**		PO.1.3

Control Identifier	Control (or Control Enhancement) Name	C-SCRM Baseline	SSDF V1.1 Task(s)
SA-9(3)	**External System Services | Establish and Maintain Trust Relationship with Providers**		PO.1.3, PW.4.4
SA-10	**Developer Configuration Management**		PO.1.3, PS.1.1, PS.3.1, RV.1.1, RV.2.2
SA-11	**Developer Testing and Evaluation**		PW.7.1, PW.7.2, PW.8.1, PW.8.2, RV.1.2, RV.2.2, RV.3.3
SA-15	**Development Process, Standards, and Tools**		PO.1.1, PO.1.2, PO.1.3, PO.3.1, PO.3.2, PO.3.3, PO.4.1, PO.4.2, PO.5.1, PO.5.2, PW.6.1, PW.6.2, RV.3.4
SA-17	**Developer Security and Privacy Architecture and Design**		PW.1.2
SR-3	**Supply Chain Controls and Processes**	x	PO.1.1, PO.1.2, PO.1.3, PS.3.2, PW.4.1, PW.4.4, RV.1.1
SR-4	**Provenance**		PO.1.3, PS.3.1, PS.3.2, PW.4.1, PW.4.4, RV.1.1
SR-5	**Acquisition Strategies, Tools, and Methods**	x	PO.1.3
SR-9	**Tamper Resistance and Detection**		PW.6.2

Attesting to Conformity with Secure Software Development Practices

NIST's attestation guidance in response to Section 4(e) outlined minimum recommendations that software purchasers should require of suppliers. That guidance was subsequently codified into the Office of Management and Budget (OMB) Memorandum M-22-18 and instructs federal acquirers to ensure that "software producers have implemented and will attest to conformity with secure software development practices."[5] The minimum elements for self-attestation in M-22-18 include:

- The software producer's name
- A description of which product or products the self-attestation statement refers to
- A statement attesting that the software producer follows secure development practices, as prescribed in NIST Guidance

Similar to Section 4(e)'s recognition that there are instances in which "minimum practices will not be sufficient,"[6] M-22-18 indicates that agencies may obtain additional artifacts (e.g., SBOMs, evidence of participation in vulnerability disclosure programs) based on criticality and other risk-based considerations, as determined by the agency.[7] SP 800-161r1 outlines such risk-based considerations for determining the appropriate degree of attestation from suppliers. Examples of risk-based considerations that may demand more robust attestation include:

- Prospective suppliers under FOCI, as outlined in Appendix E of SP 800-161r1 (e.g., a supplier or its component suppliers have headquarters; research; development; manufacturing, testing, packaging, distribution, or service facilities; or other operations in a foreign country, including a country of special concern or a foreign adversary)
- Suppliers who provide mission-critical, life safety, homeland security, critical infrastructure, or national security functions or an interdependency with another covered entity that performs such functions
- Suppliers who support high value assets or a critical system component and that have been assessed by the agency to have a risk that is high relative to the use case; assessed risk impact may or may not extend outside of the agency

[5] Office of Management and Budget. (2022). Enhancing the Security of the Software Supply Chain through Secure Software Development Practices.
[6] National Institute of Standards and Technology. (2022). Software Supply Chain Security Guidance Under Executive Order (EO) 14028 Section 4e.
[7] OMB also issued M-23-16, *Update to Memorandum 22-28*, which provides timelines for the collection of attestations. This memorandum provides supplemental guidance on the scope of M-22-18's requirements and agencies' use of POA&Ms when a software producer cannot provide the required attestation but plans to do so. In addition, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) has released the Secure Software Development Form and Instructions.

- Suppliers who require the ability to access controlled unclassified information (CUI) or classified information
- Suppliers who represent a single source of supply with limited availability of or acceptable alternatives to the product, service, or source
- Suppliers who are frequently associated with foreign adversary tactics, techniques, and procedures (TTPs); security alerts; or threat intelligence reports

In these scenarios, federal agencies should consider enhancing attestation beyond the minimum recommended practices outlined in NIST's Section 4(e) guidance and the requirements enumerated in OMB's M-22-18. Examples of enhanced attestation capabilities include:

- Supplier certifications, site visits, and/or third-party assessment and attestation
- Higher frequency and/or continuous monitoring of supplier adherence to attestation commitments
- Collection and review of lower-level artifacts, including functional and technical security controls
- Higher fidelity SBOMs, including a vendor vulnerability advisory report (VAR) at the component level

Federal agencies that seek more comprehensive attestation capabilities in higher risk scenarios should reference the evolving standards, tools, and practices guidance and Appendices D and E of SP 800-161r1.

Software Verification

NIST's third initiative in response to EO 14028 resulted in the July 2021 release of the Minimum Standards for Vendor or Developer Verification of Software. These guidelines focus primarily on developers who supply secure products and services to federal agencies. Technical descriptions and explanations for the guidelines were released as *IR 8397, Guidelines on Minimum Standards for Developer Verification of Software*, in October 2021.

At a minimum, agencies should familiarize themselves with these guidelines and ensure that applicable recommended baseline practices are being performed by their suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.

As with the security measures for critical software use, these recommended practices can be operationalized through the lens of SP 800-161r1's acquisition guidance. Table 5 outlines how the minimum software verification techniques can be used by federal agencies in conjunction with existing C-SCRM controls, control enhancements, and supplemental guidance from the lens of the acquirer.

Table 5. C-SCRM Control and Security Measure Crosswalk

Control Identifier	Control Name	EO Minimum Software Verification Technique Impact
AU-12	**Audit Record Generation**	• Expand examples of "supply chain auditable events" to include supplier attestation or third-party validation that all relevant minimum software verification techniques were performed and passed. Attestation should accompany each installation, deployment, and/or upgrade of software.
SA-3	**System Development Life Cycle**	• Integrate all applicable minimum software verification techniques into a supplier's traditional SDLC activities.
SA-4	**Acquisition Process**	• Include all applicable minimum software verification techniques into a supplier's requirements for functional properties, configuration, and implementation information, as well as any development methods, techniques, or practices that may be relevant. To differentiate between assurance activities and their effectiveness, evaluation factors should include means for weighing the inclusion of each applicable minimum software verification technique, monitoring progress, and remediating findings.

Control Identifier	Control Name	EO Minimum Software Verification Technique Impact
SA-8	**Security Engineering Principles**	• Incorporate threat modelling, fuzzing, and automation to determine the maximum possible ways that the ICT/OT product or service can be misused and abused by a supplier. • Expand the supplier's security mechanisms to include the built-in checks and protections verification technique.
SA-9	**External System Services**	• Ensure that minimum software verification techniques and results are documented alongside a supplier's cyber supply chain threats, vulnerabilities, and associated risks.
SA-10	**Developer Configuration Management**	• Mandate that the supplier's developer configuration management activities include checking software for known vulnerabilities and applying remediations and/or compensating controls to resolve or mitigate identified vulnerabilities.
SA-11	**Developer Testing and Evaluation**	• Supplement suggested C-SCRM-relevant testing with all applicable minimum software verification techniques.
SA-15	**Development Process, Standards, and Tools**	• Enhance threat modeling and vulnerability analysis activities to include the minimum software verification techniques, where applicable.
SA-22	**Unsupported System Components**	• Incorporate automated testing and built-in checks, and address code (e.g., libraries, packages, services) verification techniques to proactively identify unsupported systems or system subcomponents.
SR-6	**Supplier Assessment and Reviews**	• Augment baseline factors and assessment criteria to include a supplier's minimum software verification techniques, where applicable.
SR-9	**Tamper Resistance and Detection**	• Augment tamper resistance and detection control to include a supplier's minimum software verification techniques, where applicable.
SR-11	**Component Authenticity**	• Use automated scanning, and check included software techniques to continuously monitor configuration controls for component service and repair activities as well as anti-counterfeit scanning.

Control Identifier	Control Name	EO Minimum Software Verification Technique Impact
SI-7	**Software, Firmware, and Information Integrity**	• Expound on applicable verification tools to include all minimum software verification techniques, where applicable.
CM-3	**Configuration Change Control**	• Incorporate automated scanning, fuzzing, and other built-in checks and protections into testing, validation, and the documentation of changes to control for supplier misconfiguration risks.
CM-6	**Configuration Settings**	• Codify automated management, application, and verification activities to include all applicable minimum software verification techniques.
CM-10	**Software Usage Restrictions**	• Mandate the use of all applicable software verification techniques when utilizing open-source software components or licensed software.

Evolving Standards, Tools, and Recommended Practices

This section responds to EO 14028's mandate for NIST to gather and define evolving industry standards, tools, and recommended practices for software supply chain security in the context of federal acquirers. Given the varying levels of complexity and technical capabilities required for implementation, these concepts are presented in the Foundational, Sustaining, and Enhancing practices paradigm first introduced in SP 800-161r1upd1. Federal agencies should use these designations to prioritize the implementation of these recommended software supply chain security capabilities.

Evolving standards, tools, and recommended practices are capabilities, not requirements. They should only be implemented by federal acquirers when and where practical. The Foundational, Sustaining, and Enhancing practices designations recognize that federal department and agency acquisition and C-SCRM functions are at differing levels of program maturity.

Evolving standards, tools, and recommended practices are sourced from federal software supply chain security working groups, an array of public and private industry partnerships, and over 150 position papers submitted in advance of NIST's June 2021 Enhancing Software Supply Chain Security Workshop.

Software Bill of Materials (SBOM)

Section 10(j) of EO 14028 defines an SBOM as a "formal record containing the details and supply chain relationships of various components used in building software,"[8] similar to food ingredient labels on packaging. SBOMs offer increased transparency, provenance, and speed at which vulnerabilities[9] can be identified and remediated by federal departments and agencies. SBOMs can also indicate a developer or supplier's application of secure software development practices across the SDLC. Figure 2 illustrates an example of how an SBOM may be assembled across the SDLC.

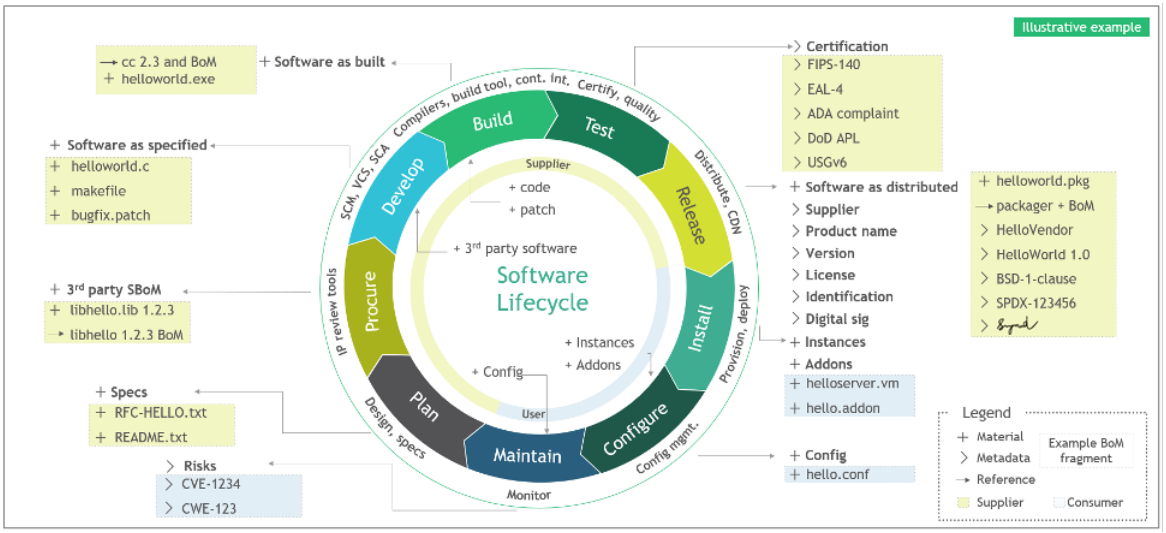

Fig. 2. Illustrative example of software life cycle and SBOM assembly line

When applicable to a procurement action, federal agencies should require their suppliers of software products and services to provide access to machine-readable SBOMs in conformance with the EO and NTIA's The Minimum Elements For a Software Bill of Materials (SBOM) by containing:

- **Data fields:** Documenting baseline information about each component that should be tracked
- **Automation support:** Allowing for scaling across the software ecosystem through automatic generation and machine readability
- **Practices and processes:** Defining the operations of SBOM requests, generation, and use

NTIA's guidance acknowledges that SBOM capabilities are currently nascent for federal acquirers and that the minimum elements are only the first key step in a process that will mature over time. As SBOMs mature, agencies should ensure that they do not

[8] Executive Office of the President. (2021). Executive Order 14028 on Improving the Nation's Cybersecurity. https://www.federalregister.gov/d/2021-10460

[9] References to vulnerabilities are inclusive of Common Weakness Enumerations (CWE) found pre-release and Common Vulnerabilities and Exposures (CVE) found post-release, as outlined in IR 8011.

deprioritize existing C-SCRM capabilities (e.g., vulnerability management practices, vendor risk assessments). SBOMs are meant to complement those capabilities rather than replace them. Federal acquirers that are unable to appropriately ingest, analyze, and act on the data that SBOMs provide will likely not improve their overall C-SCRM posture.

Federal acquirers should further consider that effectively implemented SBOMs are still subject to operational constraints. For example, SBOMs that are retroactively generated may not be able to produce the same list of dependencies used at build time. Federal acquirers should continue using the risk-based approaches outlined in SP 800-161r1 and SP 800-218 to guide their implementation of SBOMs over this period of rapid transition.

In this context, federal agencies should evaluate whether and to what extent software providers can satisfy the following recommended SBOM capabilities.

Foundational SBOM Capabilities

- Ensure that SBOMs received from third-party suppliers conform to industry standard formats to enable the automated ingestion and monitoring of versions. According to the NTIA, acceptable standard formats currently include SPDX, CycloneDX, and SWID.
- Confirm that SBOMs received from third-party suppliers meet the NTIA's Recommended Minimum Elements, including a catalog of the supplier's integration of open-source software components.
- Catalog SBOMs for all classes of software across the acquiring entities' enterprise — including purchased software, open-source software, and in-house software — by requiring sub-tier software suppliers to produce, maintain, and provide SBOMs whenever practical.
- Require software producers to maintain readily accessible and digitally signed SBOM repositories and to share SBOMs with software purchasers directly or by publishing them on a public website.

Sustaining Capabilities

- Contextualize SBOMs received from third-party suppliers with additional data elements (e.g., plug-ins, hardware components, organizational controls, and other community-provided components[10]) that inform the risk posture of the acquiring entity.
- Confirm that SBOMs received from third-party suppliers detail the supplier's integration of commercial software components.
- Integrate vulnerability detection capabilities with the acquiring entity's SBOM repositories to enable automated alerting for applicable cybersecurity risks throughout the supply chain.[11]

Enhancing Capabilities

- Ensure that third-party suppliers continuously enrich SBOM data with a VAR.
- Acquiring entities should develop risk management and measurement capabilities to dynamically monitor the impacts of SBOM-related VARs. Acquiring organizations should align with asset inventories for further risk exposure and criticality calculations.[12]
- Perform binary decomposition of software installation packages to generate SBOMs if no vendor-supplied SBOM is available (e.g., legacy software), when technically and legally feasible.[13]

[10] GitLab. (2021). NIST Position Paper #2.
[11] Vigilant Ops. (2021). Section 4 Enhancing Software Supply Chain Security - Areas 4 and 5.
[12] Synopsys. (2021). Guidelines for software integrity chains and provenance.
[13] National Telecommunications and Information Administration. (2021). The Minimum Elements For a Software Bill of Materials
(SBOM). https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf

Enhanced Vendor Risk Assessments

The EO creates higher standards for software verification techniques and other software supply chain controls. Therefore, additional scrutiny is being placed on the software that the vendors produce, as well as the business entities within a given software supply chain that may sell, distribute, store, or otherwise have access to the software code. Federal agencies that seek to enhance their assessment of supplier software supply chain controls can perform additional scrutiny on vendor SDLC capabilities, security postures, and risks associated with FOCI.

The following capabilities provide recommended vendor risk assessment and attestation capabilities beyond those outlined in Section 4 of EO 14028.

Foundational Capabilities

- Assess and analyze vendors who utilize open-source data and (as resources permit) commercially available third-party assessment and security ratings platforms. Acquirers with access to confidential information may further supplement these outside-in analyses.
- Require vendors to periodically self-attest to adopting practices that conform to the applicable requirements of SP 800-218, such as Produce Well-Secured Software's (PW) *Test Executable Code to Identify Vulnerabilities and Verify Compliance with Security Requirements*.
- Automatically verify hashes/signatures for all vendor-supplied software installation and updates, where feasible.[14]

Sustaining Capabilities

- Require vendors to submit third-party attestation that they conform to the applicable requirements of SSDF V1.1.
- Extend foundational capability recommendations to subsidiary suppliers designated within outside-in analyses and/or SBOMs, to the extent feasible.
- Include flow-down requirements to sub-tier suppliers in agreements that pertain to the secure development, delivery, operational support, and maintenance of software.
- Prioritize or mandate the use of suppliers who provide a software security label or data sheet that includes information about the software itself, the tools and technologies used to build the software, security standards and controls, the tools and processes that govern the software, and information on the

[14] Enduring Security Framework. (2021). User Group's Overview of the Top Supply Chain Threats. https://www.nsa.gov/About/Cybersecurity-Collaboration-Center/Cybersecurity-Partnerships/ESF/

qualifications and skills of the key personnel involved in building the software for all provided products, where possible.[15]

Enhancing Capabilities

- Require vendors to periodically submit third-party attestation that they conform to the applicable requirements of SSDF V1.1 and the enhancing SSDLC capabilities (e.g., automated build deployments, pre-production testing, automatic rollbacks, and staggered production deployments), including low-level artifacts, where feasible and appropriate.[16]
- Enforce just-in-time credentials for supplier build systems.[17]

[15] Contrast Security. (2021). 5. Guidelines for software integrity chains and provenance.
[16] Amazon Web Services. (2021). NIST June 2021 EO Workshop Submission.
[17] Enduring Security Framework. (2021). User Group's Overview of the Top Supply Chain Threats. https://www.nsa.gov/About/Cybersecurity-Collaboration-Center/Cybersecurity-Partnerships/ESF/

Open-Source Software Controls

As stated in the EO, "ensuring and attesting, to the extent practicable, to the integrity and provenance of open-source software components used within any portion of a product"[18] is a central driver behind many flagship initiatives like the SBOM. Though organizations should enforce formal baseline software supply chain security controls regardless of where and how code is developed, the risks of using open-source or community-developed software are unique. Open-source projects are diverse, numerous, and use a wide range of operating models. Many of these projects' provenance, integrity, support maintenance, and other underlying functions are not well-understood or easy to discover and vary from one project to the next.

Open-source software components are pervasive, and federal agencies should understand their suppliers' usage of open-source software components by considering the capabilities recommended below.

Foundational Capabilities

- Utilize Protect the Software (PS) and Respond to Vulnerabilities (RV) guidance in SSDF V1.1 to identify any publicly known vulnerabilities of supplied open-source software components (e.g., Software Composition Analysis [SCA]).
- Apply procedural and technical controls to ensure that open-source software components are acquired via secure channels from trustworthy repositories.[19]

Sustaining Capabilities

- Supplement SCA source code-based reviews with binary software composition analyses to identify vulnerable components in supplied binaries or images that could have been introduced during build and run activities to ascertain whether vulnerabilities are applicable to the end product and to verify the contents of the end product prior to implementation, including verifying the applied compiler options. These tools can also be utilized to determine whether in-house developed codebases leverage vulnerable open-source software components.[20]
- Set up and maintain one or more repositories and/or libraries of open-source software components that developers may utilize as part of a robust continuous integration/continuous delivery (CI/CD) pipeline, in accordance with SSDF V1.1.

---

[18] Executive Office of the President. (2021). Executive Order 14028 on Improving the Nation's Cybersecurity. https://www.federalregister.gov/d/2021-10460

[19] Broadcom and Symantec (A Division of Broadcom). (2021). Position Paper on Standards and Guidelines to Enhance Software Supply Chain Security.

[20] BlackBerry. (2021). Position Paper Secure Software Development Environment and Testing Software Code.

This can include a repository to host sanctioned and vetted open-source components.

Enhancing Capabilities

- Prioritize the use of programming languages and frameworks that have built-in guardrails to proactively mitigate common types of vulnerabilities.[21]
- Automate the pipeline of collecting, storing, and scanning open-source software components to designated, hardened internal repositories and/or sandboxes prior to introduction into development environments.

[21] Google. (2021). High-Confidence, Scalable Secure Development.

Vulnerability Management

Vulnerabilities are discovered in a variety of sources. Software developers may find security bugs in already-deployed code. Security researchers and penetration testers may find vulnerabilities by scanning or manually testing software and accessible systems. Effectively identifying, triaging, remediating, and reporting vulnerabilities are central pillars of the EO. In its discussion of Zero Trust Architecture, the EO recognizes that the discovery of vulnerabilities is inevitable, and federal agencies should focus on managing those vulnerabilities efficiently and comprehensively.

Federal agencies should adhere to NIST's existing Vulnerability Disclosure Program guidance in SP 800-216, *Recommendations for Federal Vulnerability Disclosure Guidelines*, which addresses reporting, coordinating, publishing, and receiving information about security vulnerabilities. Agencies should require their software suppliers to participate in a Vulnerability Disclosure Program or monitor them as potential risks. Agencies should also require a range of supplier activities and capabilities that enable the comprehensive and timely management of vulnerabilities. For example, agencies may require that suppliers disclose whether provided software components are vulnerable to exploitation through a vulnerability advisory report in an automated and machine-readable format (e.g., Vulnerability Exploitability eXchange [VEX]). Agencies should be able to accept vulnerability advisories in an automated format.

Per [ISO/IEC 29147], the elements of a vulnerability advisory report include:

- Identifier
- Date/time
- Title
- Overview
- List of affected products
- Description of intended audience
- Description of the vulnerability
- Impact
- Severity
- Remediation
- References
- Discovery credit
- Contact information
- Revision history
- Terms of use

Foundational Capabilities

- Acquiring entities should ensure that third-party suppliers demonstrate their adoption of SSDF V1.1 in the development of software (e.g., effective change

control, automation, robust CI/CD, and DevSecOps practices to mitigate and report common vulnerabilities in accordance with RV practices). See the Attesting to Conformity With Secure Software Development Practices section for additional details.

- Acquiring entities should validate that third-party suppliers maintain a formal, publicly available means by which the public can notify the supplier of vulnerabilities.[22]
- Acquiring entities and third-party suppliers should adhere to ISO/IEC 30111, *Information technology — Security techniques — Vulnerability handling processes*, and/or ISO/IEC 29147, *Information technology — Security techniques — Vulnerability disclosure*, as appropriate.

Sustaining Capabilities

- Acquiring entities should engage third-party suppliers who participate in coordinated vulnerability disclosure (CVD) programs to support the timely remediation of vulnerabilities.[23]
- Acquiring entities should comprehensively integrate SBOMs, vulnerability databases, and other reporting mechanisms to ensure that they rapidly receive notifications of recently released vulnerabilities.

Enhancing Capabilities

- Acquiring entities should prioritize third-party suppliers who staff defined Product Security Incident Response Teams (PSIRTs) and/or internal research teams that are dedicated to the identification, triage, and remediation of vulnerabilities across the supplier's product and service suite in support of SSDF V1.1 Prepare the Organization (PO) and RV practices.[24]
- Where possible and appropriate, acquiring entities should require a vulnerability advisory report in an automated and machine-readable format (e.g., VEX).
- Acquiring entities should prioritize suppliers who utilize a formal bug bounty program to incentivize the discovery and proactive remediation of vulnerabilities before adversaries can utilize them, where feasible and legally appropriate.

[22] GitLab. (2021). NIST Position Paper: Area #5.
[23] Carnegie Mellon University Software Engineering Institute. (2021). CERT/CC Comments on Standards and Guidelines to Enhance Software Supply Chain Security (Questions 2-5).
[24] Synopsys. (2021). Guidelines for software integrity chains and provenance.

Additional Existing Industry Standards, Tools, and Recommended Practices

Though existing industry standards, tools, and recommended practices have been primarily presented through the lens of SP 800-161r1upd1, additional considerations of software supply chain security from the lens of the acquirer extend far beyond this document. Federal agencies looking for additional industry standards, tools, and recommended practices should reference the cross-industry publications listed in Table 6.

Table 6. Existing industry standards, tools, and recommended practices for acquirers

Source	Description
The BSA Framework for Secure Software: A New Approach to Securing the Software Lifecycle, Version 1.1	Offers an outcome-focused, standards-based risk management tool to help stakeholders in the software industry (e.g., developers, vendors, customers, policymakers, and others) communicate and evaluate the security outcomes associated with specific software products and services
Building Security in Maturity Model (BSIMM) Version 12	A study of existing software security initiatives across 100+ different organizations that provides a baseline of activities for software security
CISA and NIST's Defending Against Software Supply Chain Attacks	Provides an overview of software supply chain risks and recommendations on how software customers and vendors can use the C-SCRM framework and the SSDF to identify, assess, and mitigate risks
CISA's Internet of Things Security Acquisition Guidance	Provides recommendations for the acquisition function of an organization and how to apply cybersecurity and C-SCRM principles and practices throughout the acquisition life cycle when purchasing, deploying, operating, and maintaining IoT devices, systems, and services
Cyber Security & Information Systems Information Analysis Center (CSIAC) Software Assurance (SWA)	Explores different aspects of software assurance competencies that can be used to improve software assurance functions and develop or deploy assured software throughout the life cycle acquisition process
Institute for Defense Analyses (IDA), State-of-the-Art Resources (SOAR)	Enables DoD program managers (PMs) and their staff to make effective software

Source	Description
for Software Vulnerability Detection, Test, and Evaluation 2016	assurance and software supply chain risk management (SCRM) decisions, particularly when they are developing and executing their program protection plan, and inform DoD policymakers who are developing software policies
ISO/IEC 27036 Information security for supplier relationships	A multi-part standard that offers guidance on the evaluation and treatment of information risks involved in the acquisition of goods and services from suppliers
ISO/IEC 27034-1:2011 Information technology – Security techniques – Application security – Part 1: Overview and concepts	Presents an overview of application security and introduces definitions, concepts, principles, and processes that are involved in application security
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	A set of guidelines, requirements, and recommendations that address specific threats to the integrity of hardware and software COTS ICT products throughout the product life cycle
Microsoft, Security Development Life Cycle	Introduces security and privacy considerations throughout all phases of the development process to help developers build highly secure software, address security compliance requirements, and reduce development costs
National Defense Industrial Association (NDIA) Engineering for System Assurance	Provides guidance on how to build assurance into a system throughout its life cycle, as well as identifies and discusses systems engineering activities, processes, tools, and considerations to address system assurance
NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1	Voluntary guidance based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risks and designed to foster risk and cybersecurity management communications among both internal and external organizational stakeholders
IR 8259, Foundational Cybersecurity Activities for IoT Device Manufacturers	Recommends cybersecurity-related activities that manufacturers should consider performing before their IoT devices are sold to customers

Source	Description
IR 8259A, Core Device Cybersecurity Capability Baseline	Defines a baseline set of device cybersecurity capabilities that organizations should consider when confronting the challenges of IoT
Open Worldwide Application Security Project (2020) *OWASP Application Security Verification Standard 4.0.3*	Provides a basis for testing web application technical security controls and a list of requirements for secure development
OWASP Software Assurance Maturity Model (SAMM) Version 2.0	An open framework to help organizations formulate and implement a strategy for software security that is tailored to the specific risks that the organization faces
Software Assurance Forum for Excellence in Code (SAFECode), Practical Security Stories and Security Tasks for Agile Development Environments	Translates secure development practices into a language and format that agile practitioners can more readily act upon as part of a standard agile methodology
SAFECode, Fundamental Practices for Secure Software Development: Essential Elements of a Secure Development Life Cycle Program, Third Edition	A best practices guide written by SAFECode members to help software developers, development organizations, and technology users initiate or improve their software assurance programs and encourage the industry-wide adoption of fundamental secure development practices
SAFECode, Software Integrity Controls: An Assurance-Based Approach to Minimizing Risks in the Software Supply Chain	Examines the software integrity element of software assurance and provides insight into effective controls for minimizing the risk that intentional and unintentional vulnerabilities could be inserted into the software supply chain
SAFECode, Managing Security Risks Inherent in the Use of Third-Party Components	Provides a blueprint for how to identify, assess, and manage the security risks associated with the use of third-party components
SAFECode, Tactical Threat Modeling	Provides guidance on the process of threat modeling and the “generic” framework in which a successful threat-modeling effort can be conducted
SP 800-53r5, **Security and Privacy Controls for Federal Information Systems and Organizations**	Provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters,

Source	Description
	structural failures, foreign intelligence entities, and privacy risks
SP 800-53Ar4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans	Provides a set of procedures for assessing security and privacy controls that are employed in federal information systems and organizations
SP 800-53B, Control Baselines for Information Systems and Organizations	Provides three security control baselines (i.e., low-impact, moderate-impact, and high-impact) and a privacy baseline that is applied to systems irrespective of impact level
SP 800-160v1r1, **Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems**	Addresses the engineering-driven perspective and actions necessary to develop more defensible and survivable systems, including the machine, physical, and human components that compose the systems and the capabilities and services delivered by those systems

Frequently Asked Questions

Why is this guidance no longer a part of SP 800-161r1?

NIST's response to EO 14028 Section 4(c) was initially developed and contained within Appendix F of SP 800-161r1upd1, to ensure that it received sufficient public comment and review within the EO-designated timelines. Though traceability with Appendix F remains in SP 800-161r1, the content has been relocated online to:

- Allow for colocation with related EO 14028 guidance under NIST's purview
- Enable updates to more areas of evolving guidance without directly impacting SP 800-161r1
- Provide traceability and linkage with other NIST web-based assets as and when they move online to encourage dynamic and interactive engagement with the public

How does this guidance address Sections 4(c) and (d) of EO 14028?

This guidance consolidates existing industry standards, tools, and recommended practices from SP 800-161r1 and subsequent guidance on NIST's EO 14028 webpage. It also provides evolving standards, tools, and recommended practices from over 150 position papers submitted in advance of NIST's June 2021 Enhancing Software Supply Chain Security Workshop, federal software supply chain security working groups, and an array of public and private industry partnerships.

I have software procurement-related responsibilities (e.g., acquisition and procurement officials, technology professionals) for my agency and suspect that I may need to provide enhanced attestation guidance based on the risk that a producer poses to my agency. What guidance should I reference to adequately vet the purchaser?

Consult SP 800-161r1, Section 3 to contextualize attestation activities utilizing a risk-based approach. Additional guidance may be found in Appendix D in the form of vendor risk assessment templates and Appendix E, which expounds on FOCI and other higher risk scenarios.

How does one determine whether or not a supplier is under Foreign Ownership, Control, or Influence (FOCI)?

Per Appendix E of SP 800-161r1, FOCI is defined as:

> …ownership of, control of, or influence over the source or covered article(s) by a foreign interest (foreign government or parties owned or controlled by a foreign government, or other ties between the source and a foreign

government) that has the power, direct or indirect, whether or not exercised, to direct or decide matters affecting the management or operations of the company.

Where can I learn more about Cyber Supply Chain Risk Management (C-SCRM)?

See NIST's flagship C-SCRM guidance, SP 800-161r1. The publication's broader C-SCRM control guidance, risk assessment approaches, and supplier templates further guide implementation and provide recommendations for organizations seeking to iteratively improve their C-SCRM programs.

NIST'S RESPONSE TO SECTION 4(d)

EO 14028 Section 4(d) stipulates that software supply chain security guidance and associated publications must be regularly maintained. NIST recognizes that this discipline is rapidly evolving and that many topics, capabilities, and guidance discussed herein will similarly evolve. As such, NIST will apply the policies and processes for the life cycle management of cryptographic standards and guidelines described in IR 7977, to periodically review and update the guidelines described in Section 4(d) of EO 14028.

NIST's Framework Update Process describes how NIST:

1. Continually and regularly engages in community outreach activities by attending and participating in meetings, events, and roundtable dialogs
2. Solicits direct feedback from industry through requests for information (RFI), requests for comments (RFC), and NIST team email
3. Observes and monitors relevant resources and references that are published by government, academia, and industry, including descriptions of Framework use

Together, IR 7977 and the Framework Update Process illustrate the procedures that will be followed to periodically review and update the guidelines described in Section 4(d).

What changes were made to this guidance alongside the SP 800-161r1 Errata Update?

Following the initial publication of this guidance, OMB released M-22-18, which outlines additional guidance for federal departments and agencies seeking to obtain attestations of secure software development practices from their third-party suppliers. The section on Attesting to Conformity With Secure Software Development Practices has been revised to reflect this development.

Additional revisions have been made across the Evolving Standards, Tools, and Recommended Practices section to clarify roles and responsibilities for organizations seeking to implement a recommended practice.