

# Software Security in Supply Chains

[Introduction](#)

[Guidance, Purpose, Scope, and Audience](#)

[EO-Critical Software and Security Measures for EO-Critical Software](#)

[Software Cybersecurity for Producers and Users](#)

[Attesting to Conformity with Secure Software Development Practices](#)

[Software Verification](#)

[Evolving Standards, Tools, and Recommended Practices](#)

[Software Bill of Materials \(SBOM\)](#)

[Enhanced Vendor Risk Assessments](#)

[Open Source Software Controls](#)

[Vulnerability Management](#)

[Additional Existing Industry Standards, Tools, and Recommended Practices](#)

[Frequently Asked Questions \(FAQs\)](#)

# Introduction

The [Executive Order \(EO\) on Improving the Nation's Cybersecurity](#) released on May 12, 2021 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<sup>1</sup> practices are sourced from:

- NIST’s foundational C-SCRM guidance, [SP 800-161, Rev. 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations](#);
- [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 800-161, Rev. 1.

## Existing Standards, Tools, and Recommended Practices

Existing industry standards, tools, and recommended practices are sourced from NIST’s [SP 800-161, Rev. 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations](#), and its interrelation with guidance published by NIST 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 800-161, Rev. 1, controls upon their suppliers and – where feasible – adopt new software supply chain security recommendations that previously fell outside of the explicit scope of SP 800-161, Rev. 1, in the context of EO 14028.

---

<sup>1</sup> 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 providing recommendations to both public and private organizations.

- **Existing standards, tools, and recommended practices.** This guidance provides direction to federal agency acquirers on how to augment existing SP 800-161, Rev. 1, controls in accordance with EO 14028. It focuses on 1) EO-critical Software, 2) Software Cybersecurity for Producers and Users, 3) Software Verification, and 4) Cybersecurity Labeling for Consumers: 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 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 800-161, Rev. 1, as a source of reference.

# 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 [Executive Order \(EO\) 14028](#). It calls for applying the controls in [SP 800-161, Rev. 1](#), 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. 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 the relationship map below, Section 4(e) and the associated [SP 800-218, \*Secure Software Development Framework \(SSDF\) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities\*](#), contains guidance on secure software produced or developed in-house by federal agencies or by third-party suppliers.

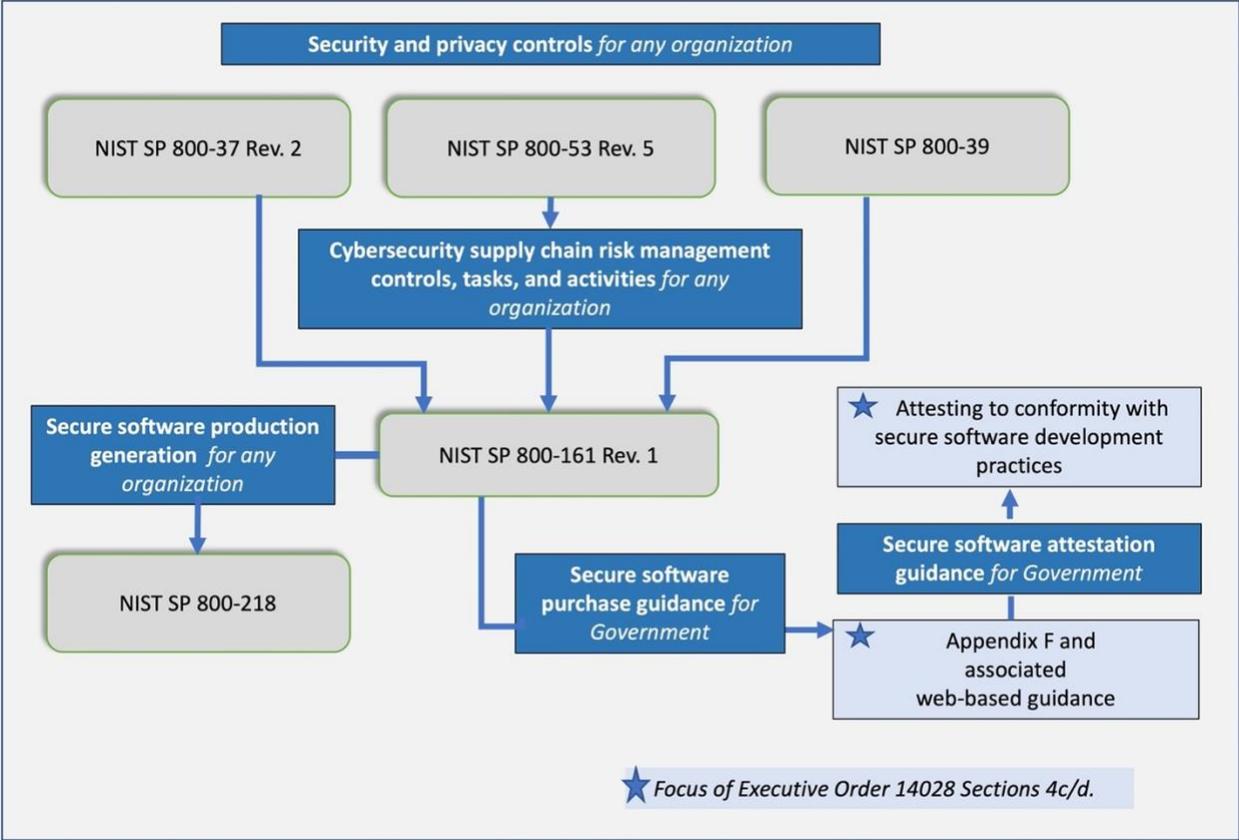


Figure 1 - Relationship map between SSDF V1.1 and EO 14028, Section 4(d)

# EO-Critical Software and Security Measures for EO-Critical Software

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.”<sup>2</sup>

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

## Definition of EO-Critical Software

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

Table F-1: Impacts of EO-critical software definition on SP 800-161, Rev. 1, guidance for Federal Agencies

Section Identifier	Section Title	EO-Critical Definition Impact
2	<b>Integration of C-SCRM into Enterprise-wide Risk Management</b>	<ul style="list-style-type: none"> <li>Enhance SP 800-39’s Assess risk step with EO-critical risk definitions when considering software supply chain components and suppliers.</li> </ul>
2.3	<b>Multilevel Risk Management</b>	<ul style="list-style-type: none"> <li>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.</li> </ul>
3.1	<b>C-SCRM in Acquisition</b>	<ul style="list-style-type: none"> <li>Ensure that groupings accommodate EO-critical suppliers when segmenting the organization’s supplier relationships and contracts.</li> <li>Codify function-based software criticality definitions during the ‘plan procurement’ step, and incorporate EO-critical concepts when justifying the level of criticality.</li> </ul>
3.4	<b>C-SCRM Key Practices</b>	<ul style="list-style-type: none"> <li>Integrate context-based criticality concepts within the Foundational Practices’ measurement</li> </ul>

<sup>2</sup> National Institute of Standards and Technology. (2021). [Definition of Critical Software Under Executive Order \(EO\) 14028](#).

Section Identifier	Section Title	EO-Critical Definition Impact
		<p>of supplier criticality and the utilization of supplier risk assessments.</p> <ul style="list-style-type: none"> <li>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).</li> </ul>
<b>Appendix A</b>	<b>C-SCRM Security Controls</b>	<ul style="list-style-type: none"> <li>Extend EO-critical definition considerations to ICT/OT related service providers, where applicable</li> </ul>
<b>Appendix C</b>	<b>Risk Exposure Framework</b>	<ul style="list-style-type: none"> <li>Incorporate EO-critical definition components when determining the organization’s acceptable level of risk, particularly within the context of system criticality assessments.</li> </ul>
<b>Appendix D</b>	<b>C-SCRM Templates</b>	<ul style="list-style-type: none"> <li>Account for EO-critical definitions when considering the automated generation of C-SCRM plan elements, such as supply chain component criticality.</li> </ul>
<b>Appendix E</b>	<b>FASCSA</b>	<ul style="list-style-type: none"> <li>Account for risk factors associated with EO-critical definitions when identifying, assessing, and responding to supply chain risk.</li> </ul>
<b>Appendix G</b>	<b>C-SCRM Activities in the Risk Management Process</b>	<ul style="list-style-type: none"> <li>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).</li> </ul>

## Security Measures (SM) for EO-Critical Software Use

NIST published “[Security Measures for ‘EO-Critical Software’ Use Under Executive Order \(EO\) 14028](#)” in July 2021. Software supply chain security measures are essential for internal decision-making and for supplier oversight. Federal agencies must recognize their status as critical players in the software supply chain and should, at a minimum, implement the same security controls internally 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.

The table below outlines the mappings and coverage of the EO’s security measures across SP 800-161, Rev. 1, controls, control enhancements, and supplemental guidance outlined in the main body of this document. Many of these are included in the

C-SCRM controls baseline.

EO Security Measures and their associated NIST SP 800-161, Rev. 1, 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 to SP 800-161, Rev. 1, controls should use the below table to aid in conforming with EO Security Measures and to ensure their effective application across the software supply chain and acquisition life cycle.

Table F-2: C-SCRM Control and Security Measure 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 <sup>2</sup>	x <sup>3</sup>	2.2, 3.3
AC-17	Remote Access	X	2.4
AT-2	Literacy Training and Awareness <sup>2</sup>	X <sup>3</sup>	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 <sup>2</sup>	X <sup>3</sup>	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

<sup>3</sup> While the base control is not addressed within SP 800-161, Rev. 1, the topic at large is addressed through supplemental guidance provided for control enhancements to the base control within SP 800-161, Rev.1.

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

The measures are intended to secure the use of deployed EO-critical software in federal agencies’ operational environments. 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 Executive Order (EO) 14028” falls outside of the scope of SP 800-161, Rev. 1. 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.”<sup>4</sup>[\[3\]](#) Though relevant to sound C-SCRM practices, controls related to Security Measure 2.5 are not included in SP 800-161, Rev. 1, 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 the table below.

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

---

<sup>4</sup> National Institute of Standards and Technology. (2021). [Security Measures for “EO-Critical Software” Use Under Executive Order \(EO\) 14028](#).

this table to accelerate conformance or refer directly to “Security Measures for ‘EO-Critical Software’ Use Under Executive Order (EO) 14028.”

Table F-3: C-SCRM Control and Security Measure Crosswalk

<b>Control Identifier</b>	<b>Control (or Control Enhancement) Name</b>	<b>C-SCRM Baseline</b>	<b>EO Security Measure</b>
<b>AU-4</b>	<b>Audit Log Storage Capacity</b>	N/A	4.1
<b>AU-5</b>	<b>Response to Audit Logging Process Failures</b>	N/A	4.1
<b>AU-8</b>	<b>Timestamps</b>	N/A	4.1
<b>AU-11</b>	<b>Audit Record Retention</b>	N/A	4.1
<b>CA-7</b>	<b>Continuous Monitoring</b>	N/A	3.2, 3.3, 4.1
<b>CP-9</b>	<b>System Backup</b>	N/A	2.5
<b>CP-10</b>	<b>System Recovery and Reconstitution</b>	N/A	2.5
<b>SC-2</b>	<b>Separation of System and User Functionality</b>	N/A	1.3
<b>SC-7(15)</b>	<b>Boundary Protection   Networked Privileged Accesses</b>	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 [SSDF V1.1](#) (see below).

A notable exception in NIST’s response to 4(e) is its [Attesting to Conformity with Secure Software Development Practices](#), which – as the name implies – 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 to federal agency acquirers seeking to use a common vocabulary with suppliers during acquisition and to augment their existing C-SCRM controls. The table below identifies likely areas of impact across supply chain acquisition and procurement activities.

Table F-4: C-SCRM Control 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

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

# Attesting to Conformity with Secure Software Development Practices

NIST's attestation guidance in response to Section 4(e) outlines four minimum recommendations that software purchasers should require from suppliers. The guidance recognizes that there are instances in which "these minimum practices will not be sufficient"<sup>5</sup> due to agency-specific risk-based considerations.

SP 800-161, Rev. 1. outlines an array of such risk-based considerations that federal agency acquirers should consider when determining the appropriate degree of attestation from suppliers. Examples of risk-based considerations that demand more robust attestation include:

- Prospective suppliers under Foreign Ownership, Control, or Influence (FOCI), as outlined in Appendix E of SP 800-161, Rev. 1 (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 performing or essential to 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
- 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 four minimum recommended practices outlined in Attesting to Conformity with Secure Software Development Practices guidance. 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

---

<sup>5</sup> National Institute of Standards and Technology. (2022). [Software Supply Chain Security Guidance Under Executive Order \(EO\) 14028 Section 4e.](#)

- Collection and review of lower-level artifacts, including functional and technical security controls
- Higher fidelity SBOMs, including vendor vulnerability disclosure reports at the component level

Federal agencies seeking more comprehensive attestation capabilities in higher risk scenarios should reference the evolving standards, tools, and practices guidance and Appendices D and E of SP 800-161, Rev.1.

# Software Verification

The third initiative launched by NIST in response to EO 14028 resulted in the [Minimum Standards for Vendor or Developer Verification of Software](#). These guidelines, released in July 2021, focus primarily on developers supplying secure products and services to federal agencies. Technical descriptions and explanations to the guidelines were released as [NISTIR 8397, Guidelines on Minimum Standards for Developer Verification of Software](#), in October 2021.

At a minimum, agencies should familiarize themselves with these guidelines and take action to ensure 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 800-161, Rev. 1, acquisition guidance. Table F-5 outlines how the minimum software verification techniques can be used by federal agencies to enhance existing C-SCRM controls, control enhancements, and supplemental guidance from the lens of the acquirer.

Table F-5: C-SCRM Control and Security Measure Crosswalk

Control Identifier	Control Name	EO Minimum Software Verification Technique Impact
AU-12	<b>Audit Record Generation</b>	<ul style="list-style-type: none"> <li>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.</li> </ul>
SA-3	<b>System Development Life Cycle</b>	<ul style="list-style-type: none"> <li>Integrate all applicable minimum software verification techniques into a supplier’s traditional SDLC activities.</li> </ul>
SA-4	<b>Acquisition Process</b>	<ul style="list-style-type: none"> <li>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, and remediating findings.</li> </ul>

<b>Control Identifier</b>	<b>Control Name</b>	<b>EO Minimum Software Verification Technique Impact</b>
<b>SA-8</b>	<b>Security Engineering Principles</b>	<ul style="list-style-type: none"> <li>• 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.</li> <li>• Expand the supplier’s security mechanisms to include the built-in checks and protections verification technique.</li> </ul>
<b>SA-9</b>	<b>External System Services</b>	<ul style="list-style-type: none"> <li>• Ensure that minimum software verification techniques and results are documented alongside a supplier’s cyber-supply chain threats, vulnerabilities, and associated risks.</li> </ul>
<b>SA-10</b>	<b>Developer Configuration Management</b>	<ul style="list-style-type: none"> <li>• Mandate that the supplier’s developer configuration management activities include checking software for known vulnerabilities, as well as the application of remediations and/or compensating controls to resolve or mitigate identified vulnerabilities.</li> </ul>
<b>SA-11</b>	<b>Developer Testing and Evaluation</b>	<ul style="list-style-type: none"> <li>• Supplement suggested C-SCRM-relevant testing with all applicable minimum software verification techniques.</li> </ul>
<b>SA-15</b>	<b>Development Process, Standards, and Tools</b>	<ul style="list-style-type: none"> <li>• Enhance threat modeling and vulnerability analysis activities to include the minimum software verification techniques, where applicable.</li> </ul>
<b>SA-22</b>	<b>Unsupported System Components</b>	<ul style="list-style-type: none"> <li>• 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.</li> </ul>
<b>SR-6</b>	<b>Supplier Assessment and Reviews</b>	<ul style="list-style-type: none"> <li>• Augment baseline factors and assessment criteria to include a supplier’s minimum software verification techniques, where applicable.</li> </ul>
<b>SR-9</b>	<b>Tamper Resistance and Detection</b>	<ul style="list-style-type: none"> <li>• Augment tamper resistance and detection control to include a supplier’s minimum software verification techniques, where applicable.</li> </ul>
<b>SR-11</b>	<b>Component Authenticity</b>	<ul style="list-style-type: none"> <li>• Use automated scanning, and check included software techniques to continuously monitor configuration control for component service and repair activities as well as anti-counterfeit scanning.</li> </ul>

Control Identifier	Control Name	EO Minimum Software Verification Technique Impact
SI-7	<b>Software, Firmware, and Information Integrity</b>	<ul style="list-style-type: none"> <li>• Expound on applicable verification tools to include all minimum software verification techniques, where applicable.</li> </ul>
CM-3	<b>Configuration Change Control</b>	<ul style="list-style-type: none"> <li>• 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.</li> </ul>
CM-6	<b>Configuration Settings</b>	<ul style="list-style-type: none"> <li>• Codify automated management, application, and verification activities to include all applicable minimum software verification techniques.</li> </ul>
CM-10	<b>Software Usage Restrictions</b>	<ul style="list-style-type: none"> <li>• Mandate the use of all applicable software verification techniques when utilizing open source software components or licensed software (which may also apply to some open source software components).</li> </ul>

# Evolving Standards, Tools, and Recommended Practices

C-SCRM and software supply chain security disciplines have evolved rapidly in recent years. The release of [EO 14028](#), subsequent discussions, and cross-industry publications have brought many of these evolutions to the fore. This section responds to EO 14028's mandate for NIST to gather and define those evolving industry standards, tools, and recommended practices in software supply chain security.

As with the existing standards, tools, and recommended practices provided above, these evolving concepts are tailored to 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 800-161, Rev. 1](#). Federal agencies should use these designations to prioritize the implementation of these recommended leading software supply chain security capabilities.

Evolving standards, tools, and recommended practices are capabilities, not requirements, and are only to be implemented by federal acquirers when and where practical. The Foundational, Sustaining, and Enhancing practices designations recognize that federal departments and agencies 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<sup>6</sup>” similar to food ingredient labels on packaging. SBOMs hold the potential to provide increased transparency, provenance, and speed at which vulnerabilities<sup>7</sup> can be identified and remediated by federal departments and agencies. SBOMs can also be indicative of a developer or suppliers’ application of secure software development practices across the SDLC. Figure F-1 illustrates an example of how an SBOM may be assembled across the SDLC.

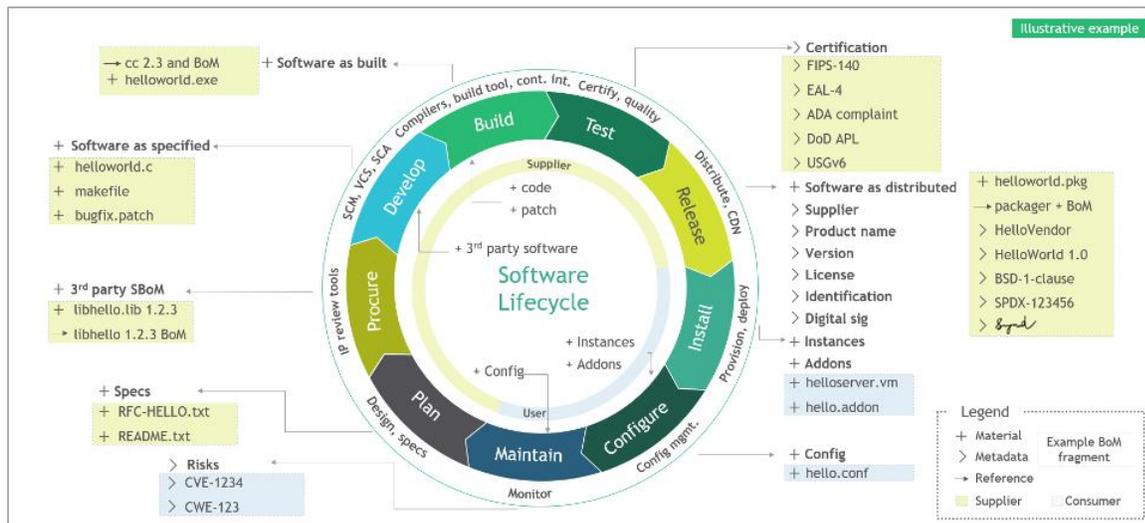


Figure 2 - Illustrative Example of Software Life Cycle and Bill of Materials Assembly Line

Federal agencies should ensure that their suppliers of software products and services are able to produce 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

<sup>6</sup> Executive Office of the President. (2021). Executive Order 14028 on Improving the Nation's Cybersecurity. <https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity>

<sup>7</sup> 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 [NISTIR 8011 Vol. 4, Automation Support for Security Control Assessments: Software Vulnerability Management](#).

NTIA’s guidance acknowledges that SBOM capabilities are currently nascent for federal acquirers and that the minimum elements are but “a key, initial step in the SBOM process that will advance and mature over time”. As SBOMs mature, agencies should ensure they do not deprioritize existing C-SCRM capabilities (e.g., vulnerability management practices, vendor risk assessments) under the mistaken assumption that SBOM replaces these activities. SBOMs and the improved transparency that they are meant to provide for federal acquirers are a complementary, not substitutive, capability. 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. Though this constraint may diminish over time, federal acquirers should continue using the risk-based approaches outlined in SP 800-161 Rev. 1 and SP 800-218 to guide their implementation of SBOMs over this rapid period of transition.

In his context, federal agencies should consider, where possible and applicable, the following recommended SBOM capabilities:

## Foundational Capabilities

- Ensure that SBOMs conform to industry standard formats to enable the automated ingestion and monitoring of versions. According to the National Telecommunications and Information Administration, acceptable standard formats currently include [SPDX](#), [CycloneDX](#), and [SWID](#).
- Provide SBOMs that meet the NTIA’s Recommended Minimum Elements, including a catalog of the supplier’s integration of open source software components.
- Ensure that SBOMs are available for all classes of software – including purchased software, open source software, and in-house software – by requiring sub-tier software suppliers to produce, maintain, and provide SBOMs whenever practical.
- Maintain readily accessible and digitally signed SBOM repositories, and share SBOMs with software purchasers directly or by publishing them on a public website.

## Sustaining Capabilities

- Contextualize SBOM data with additional data elements that inform the risk posture of the acquiring entity. Additional data elements include plug-ins, hardware components, organizational controls, and other community-provided components<sup>8</sup>.
- Integrate vulnerability detection with SBOM repositories to enable automated alerting for applicable cybersecurity risks throughout the supply chain<sup>9</sup>.
- Ensure that current SBOMs detail the supplier's integration of commercial software components.
- Maintain vendor vulnerability disclosure reports at the SBOM component level.

## Enhancing Capabilities

- Develop risk management and measurement capabilities to dynamically monitor the impact of SBOMs' vulnerability disclosures on the acquiring organization. Align with asset inventories for further risk exposure and criticality calculations<sup>10</sup>.
- Perform binary decomposition of software installation packages to generate SBOMs when no vendor-supplied SBOM is available (e.g., legacy software), when technically and legally feasible<sup>11</sup>.

---

<sup>8</sup> GitLab. (2021). [NIST Position Paper #2](#).

<sup>9</sup> [Vigilant Ops. \(2021\). Section 4 Enhancing Software Supply Chain Security - Areas 4 and 5](#).

<sup>10</sup> Synopsys. (2021). [Guidelines for software integrity chains and provenance](#).

<sup>11</sup> 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](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 posture, and risks associated with Foreign Ownership, Control, or Influence (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 [SSDF V1.1](#), 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<sup>12</sup>.

## 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 should include 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

---

<sup>12</sup> 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 key personnel involved in building the software for all provided products, where possible<sup>13</sup>.

## 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<sup>14</sup>.
- Enforce just-in-time credentials for supplier build systems.<sup>15</sup>

---

<sup>13</sup> Contrast Security. (2021). [5. Guidelines for software integrity chains and provenance](#).

<sup>14</sup> Amazon Web Services. (2021). [NIST June 2021 EO Workshop Submission](#).

<sup>15</sup> 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<sup>16</sup>” 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.<sup>17</sup>

## 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 (e.g., newly discovered) vulnerabilities are applicable to the end product and to verify the contents of the end product (including verifying the applied compiler options) prior to “shipping.” These tools can also be utilized to determine whether in-house developed codebases leverage vulnerable open source software components.<sup>18</sup>

---

<sup>16</sup> Executive Office of the President. (2021). Executive Order 14028 on Improving the Nation's Cybersecurity. <https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity>

<sup>17</sup> Broadcom and Symantec (A Division of Broadcom). (2021). [Position Paper on Standards and Guidelines to Enhance Software Supply Chain Security](#).

<sup>18</sup> BlackBerry. (2021). [Position Paper Secure Software Development Environment and Testing Software Code](#).

- 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. 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.<sup>19</sup>
- 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.

---

<sup>19</sup> Google. (2021). [High-Confidence, Scalable Secure Development](#).

# Vulnerability Management

Vulnerabilities are discovered in a variety of sources. Developers of software 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 is a central pillar of the EO. In its discussion of Zero Trust architecture, the EO recognizes that the discovery of vulnerabilities is inevitable, and federal agencies' strategies should focus on how to manage those vulnerabilities efficiently and comprehensively.

Agencies should adhere to NIST's existing Vulnerability Disclosure Program guidance in [Draft NIST SP 800-216, Recommendations for Federal Vulnerability Disclosure Guidelines](#), which addresses reporting, coordinating, publishing, and receiving information about security vulnerabilities. They can also impose a range of recommended activities and capabilities from suppliers to enable more comprehensive and timely management of vulnerabilities.

## Foundational Capabilities

- Demonstrate the 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).
- Establish a formal, publicly available means by which the public can notify the supplier of uncovered vulnerabilities<sup>20</sup>.
- 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

- Adhere to a coordinated vulnerability disclosure (CVD) practice to ensure that federal departments and agencies are able to remediate vulnerabilities in a timely manner.<sup>21</sup>
- Integrate SBOMs, vulnerability databases, and reporting mechanisms to ensure that federal departments and agencies rapidly receive notification of recently released vulnerabilities.

---

<sup>20</sup> GitLab. (2021). [NIST Position Paper: Area #5](#).

<sup>21</sup> Carnegie Mellon University Software Engineering Institute. (2021). [CERT/CC Comments on Standards and Guidelines to Enhance Software Supply Chain Security \(Questions 2-5\)](#).

## Enhancing Capabilities

- Engage suppliers that staff defined product security incident response teams (PSIRT) and/or internal research teams dedicated to the identification, triage, and remediation of vulnerabilities across the supplier's product/service suite in support of SSDF V1.1 Prepare the Organization (PO) and RV practices.<sup>22</sup>
- Buy from suppliers that utilize a formal bug bounty program to incentivize the discovery and proactive remediation of vulnerabilities before adversaries are able to utilize them, where feasible and legally appropriate.

---

<sup>22</sup> 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 800-161, Rev. 1](#), additional consideration of software supply chain security from the lens of the acquirer extends far beyond this document. Federal agencies looking for additional industry standards, tools, and recommended practices should reference the cross-industry publications listed in Table F-5.

Table F-5: Existing Industry Standards, Tools, and Recommended Practices for Acquirers

Source	Description
<b>The BSA Framework for Secure Software: A New Approach to Securing the Software Lifecycle, Version 1.1</b>	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
<b>Building Security in Maturity Model (BSIMM) Version 12</b>	A study of existing software security initiatives across 100+ different organizations that provides a baseline of activities for software security
<b>CISA and NIST’s Defending Against Software Supply Chain Attacks</b>	Provides an overview of software supply chain risks and recommendations on how software customers and vendors can use the NIST Cybersecurity Supply Chain Risk Management (C-SCRM) framework and the Secure Software Development Framework (SSDF) to identify, assess, and mitigate risks
<b>CISA’s Internet of Things Security Acquisition Guidance</b>	Provides recommendations on 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
<b>Cyber Security &amp; Information Systems Information Analysis Center (CSIIAC) Software Assurance (SWA)</b>	Explores different aspects of software assurance competencies that can be used to improve software assurance functions and how to develop/deploy assured software throughout the life cycle acquisition process

Source	Description
<b>Institute for Defense Analyses (IDA), State-of-the-Art Resources (SOAR) for Software Vulnerability Detection, Test, and Evaluation 2016</b>	Written to enable DoD program managers (PMs) and their staff to make effective software 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
<b>ISO/IEC 27036 Information security for supplier relationships</b>	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
<b>ISO/IEC 27034-1:2011 Information technology – Security techniques – Application security – Part 1: Overview and concepts</b>	Presents an overview of application security and introduces definitions, concepts, principles, and processes involved in application security
<b>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</b>	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
<b>Microsoft, Security Development Life Cycle</b>	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
<b>National Defense Industrial Association (NDIA) Engineering for System Assurance</b>	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
<b>NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1</b>	Voluntary guidance based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk and designed to foster risk and cybersecurity management communications among both internal and external organizational stakeholders
<b>NISTIR 8259, Foundational Cybersecurity Activities for IoT Device Manufacturers</b>	Describes recommended activities related to cybersecurity that manufacturers should consider performing before their IoT devices are sold to customers

Source	Description
<b>NISTIR 8259A, Core Device Cybersecurity Capability Baseline</b>	Defines a baseline set of device cybersecurity capabilities that organizations should consider when confronting the challenge of the IoT
<b>Open Web Application Security Project (2020) OWASP Application Security Verification Standard 4.0.3</b>	Provides a basis for testing web application technical security controls and a list of requirements for secure development
<b>OWASP Software Assurance Maturity Model (SAMM) Version 2.0</b>	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
<b>Software Assurance Forum for Excellence in Code (SAFECode), Practical Security Stories and Security Tasks for Agile Development Environments</b>	Translates secure development practices into a language and format that Agile practitioners can more readily act upon as part of a standard Agile methodology
<b>SAFECode, Fundamental Practices for Secure Software Development: Essential Elements of a Secure Development Life Cycle Program, Third Edition</b>	Authoritative 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
<b>SAFECode, Software Integrity Controls: An Assurance-Based Approach to Minimizing Risks in the Software Supply Chain</b>	Focuses on examining the software integrity element of software assurance and provides insight into the controls that SAFECode members have identified as effective for minimizing the risk that intentional and unintentional vulnerabilities could be inserted into the software supply chain
<b>SAFECode, Managing Security Risks Inherent in the Use of Third-Party Components</b>	Provides a blueprint for how to identify, assess, and manage the security risks associated with the use of third-party components
<b>SAFECode, Tactical Threat Modeling</b>	Provides guidance on the process of threat modeling as well as the “generic” framework in which a successful threat-modeling effort can be conducted
<b>SP 800-53, Rev. 5, Joint Task Force Transformation Initiative, Security and Privacy Controls for Federal</b>	Provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other

Source	Description
<b>Information Systems and Organizations</b>	organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks
<b>SP 800-53A, Rev. 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans</b>	Provides a set of procedures for conducting assessments of security controls and privacy controls employed within federal information systems and organizations
<b>SP 800-53B, Control Baselines for Information Systems and Organizations</b>	Provides security and privacy control baselines for the Federal Government: three security control baselines (low-impact, moderate-impact, and high-impact) and a privacy baseline that is applied to systems irrespective of impact level
<b>SP 800-160 Volume 1, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems</b>	Addresses the engineering-driven perspective and actions necessary to develop more defensible and survivable systems, inclusive of 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 800-161, Rev. 1?

NIST's response to [Executive Order \(EO\) 14028](#) Section 4(c) was initially developed and contained within Appendix F of [SP 800-161, Rev. 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations](#), to ensure that it received sufficient public comment and review within the EO-designated timelines. Though traceability with Appendix F remains in SP 800-161, Rev. 1, 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 800-161, Rev. 1
- 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 the EO 14028?

This guidance consolidates existing industry standards, tools, and recommended practices from NIST's flagship Cybersecurity Supply Chain Risk Management (C-SCRM) guidance, SP 800-161, Rev. 1, as well as subsequent guidance published by NIST on its EO 14028, Improving the Nation's Cybersecurity Guidance [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 800-161, Rev. 1, 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 upon Foreign Ownership, Control, or Influence (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 800-161, Rev. 1, 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 800-161, Rev. 1. 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)**

[Executive Order \(EO\) 14028](#) Section 4(d) stipulates that the 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 [NISTIR 7977, \*NIST Cryptographic Standards and Guidelines Development Process\*](#), to guide the periodic review and updating of 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; and 3) observes and monitors relevant resources and references – including descriptions of Framework use – published by government, academia, and industry.

Together, NISTIR 7977 and the Framework Update Process illustrate the procedures that will be followed for periodic review and updating of the guidelines described in Section 4(d).