

Cherilyn Pascoe

Senior Technology Policy
Advisor | NIST

Jon Boyens

Deputy Chief, Computer
Security Division | NIST

New Guidelines for Enhancing Software Supply Chain Security Under EO 14028

NIST

NATIONAL INSTITUTE OF
STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Why Is Software Security Important?



BRIEFING ROOM

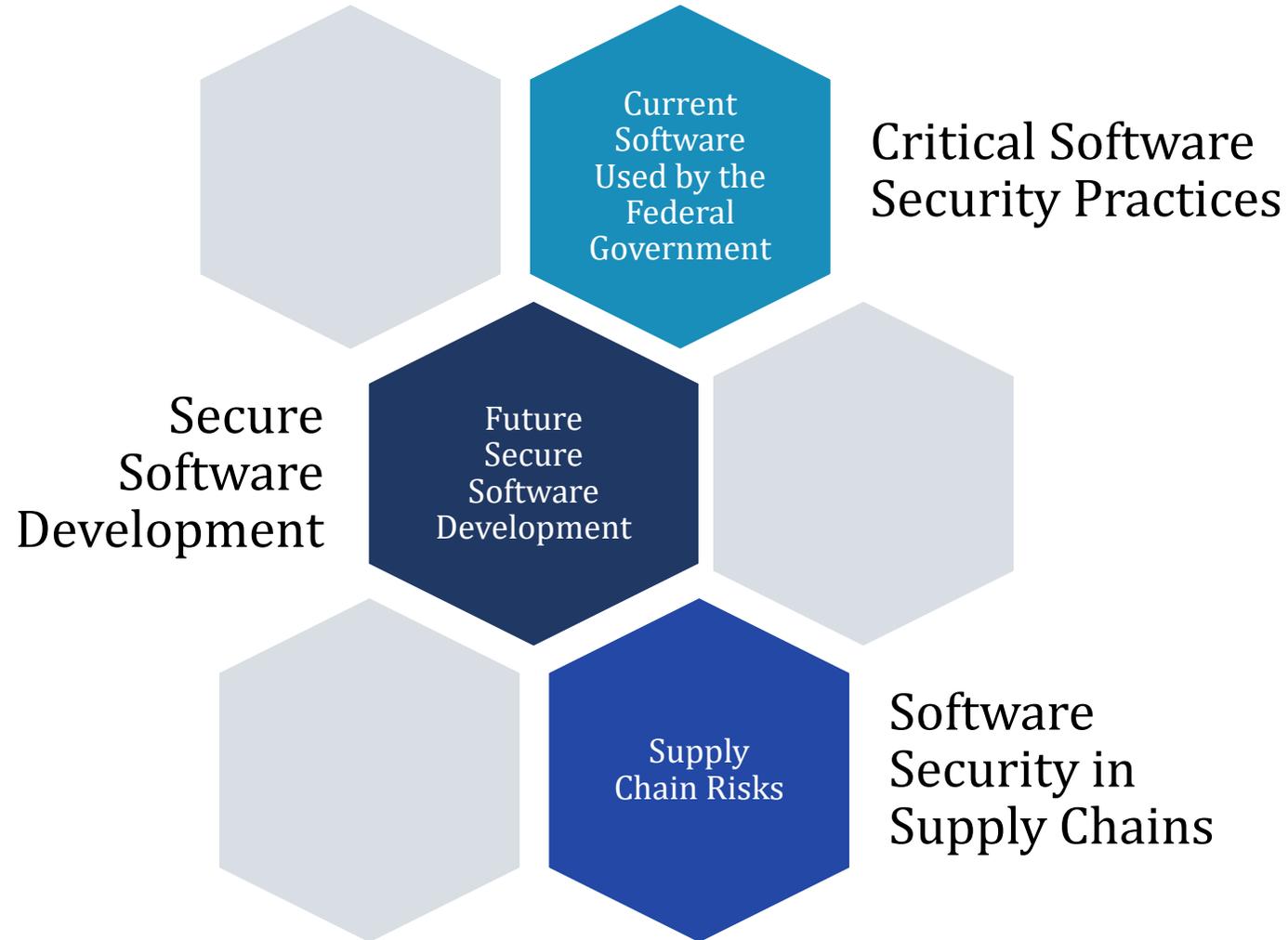
Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The

Software Security Standards & Guidance



Critical Software Security Measures: Existing Software

Critical Software Definition:

<https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/critical-software-definition>

Critical Software Security:

<https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/security-measures-eo-critical-software-use-2>



Executive Order (EO)-Critical Software Measures

Motivation

- Even though EO-critical software may be developed using recommended secure development practices, it still needs to be secured in agencies' operational environments.

Purpose & Scope

- Define “critical software” for use by federal agencies.
- Scope applies to the protection of agencies' deployed EO-critical software.
Development and acquisition are out of scope.
- The EO directs NIST to issue guidance and further directs the Office of Management and Budget (OMB) to **require** federal agencies to comply with that guidance. OMB has provided instructions on how federal agencies should identify their critical software and adopt required NIST security measures (OMB M-21-30, August 2021).

Critical Software Security Measures: Snapshot

EO-Critical Software Security Measures

Software Security Measure

Federal Government Informative References

Objective 1: **Protect** software/platforms from unauthorized access and usage

Objective 2: **Protect** the confidentiality, integrity, and availability of data

Objective 3: **Identify** and maintain to protect from exploitation

Objective 4: Quickly **detect, respond to, and recover** from threats and incidents

Objective 5: **Strengthen** understanding and performance of humans' actions that foster security

Objective 1: Protect EO-critical software and platforms from unauthorized access and usage

Security Measure 1.1: Use MFA that is **verifier impersonation-resistant for all users and administrators** of EO-critical software and EO-critical software platforms.

- **NIST**, [Cybersecurity Framework](#): PR.AC-1, PR.AC-7
- **NIST**, SP 800-53 Rev. 5, [Security and Privacy Controls for Information Systems and Organizations](#): AC-2, IA-2, IA-4, IA-5
- **CISA**, [Bad Practices](#)
-

Secure Software Development



SSDF V 1.1 (SP 800-218):
<https://csrc.nist.gov/Projects/ssdf>

Secure Software Guidance:
<https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/software-supply-chain-security-guidance>

Secure Software Development Framework (SSDF)

Motivation

- Help an organization adopt a risk-management approach to document its secure software development practices today and define its future target practices.
- OMB has required federal agencies to comply with the SSDF (OMB M-22-18, September 14, 2022).

Purpose & Scope

- Applies to software producers and software consumers regardless of size, sophistication.
- Broadly applicable to IT, IoT, and OT.

Attributes

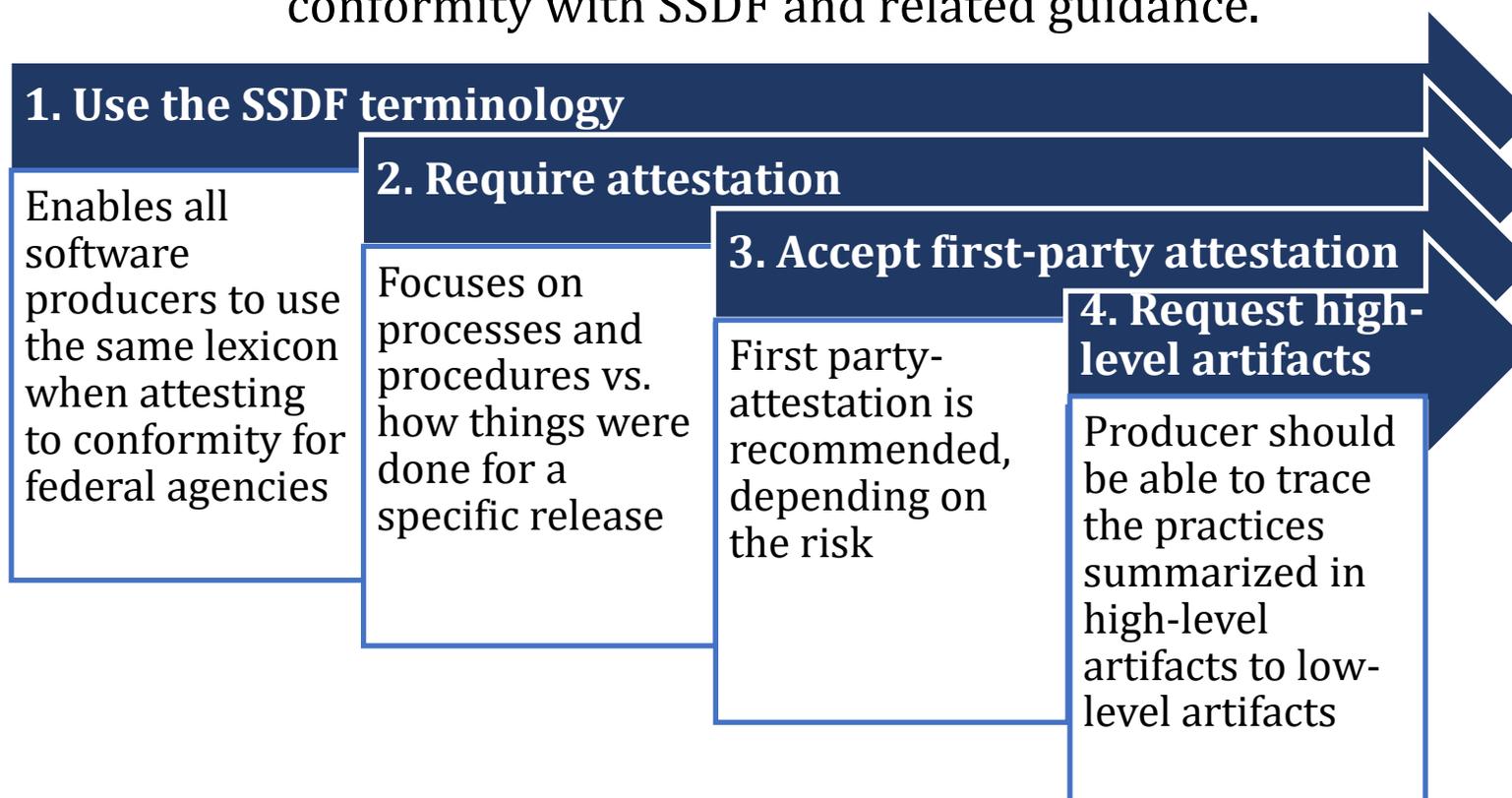
- Provides a common language and taxonomy.
- Leverages existing practices from established standards and guidance.

NIST SSDF Practice Groups



Secure Software Attestation Guidance

The EO directs NIST to issue guidance identifying practices that enhance the security of the software supply chain for producers and purchasers and then directs OMB to require federal agencies to comply with NIST guidelines with respect to software procured after the date of the order. NIST has guidance for attesting to conformity with SSDF and related guidance.



Minimum standards recommended for verification by software vendors or developers:

- **11 recommended minimums**
(+ fixing bugs!)
- **Background and supplemental information about each technique**
 - References for each technique
- **Beyond software verification (development, operation, assurance)**

- Threat modeling
- Automated testing
- Static Analysis: Use a code scanner to look for top bugs
- Static Analysis: Review for hardcoded secrets
- Dynamic Analysis: Run with built-in checks and protections
- Dynamic Analysis: Create “black box” test cases
- Dynamic Analysis: Create code-based structural test cases
- Dynamic Analysis: Use test cases created to catch previous bugs
- Dynamic Analysis: Run a fuzzer
- Dynamic Analysis: If the software might be connected to the Internet, run a web app scanner
- Check included software

Cybersecurity Supply Chain Risk Management (C-SCRM) Additional Guidance

C-SCRM Guidance:

<https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management>

Software Supply Chain Security Under the EO:

<https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-security-supply-chains>



Additional Guidance for Software Supply Chain Security (SP 800-161r1 Appendix F)

Software supply chain security concepts are a critical sub-discipline within C-SCRM.

Available online to allow for easier update to guidance.



EO through the lens of 800-161r1

EO Critical Software & Measures

Software Verification

SSDF & Attestations

Emerging concepts

Software Bill of Materials (SBOM)

Enhanced Vendor Risk Assessments

Open-Source Software Controls

Vulnerability Management



**Response
highlights |
Associated
web-based
guidance (I/II)**



Existing standards, tools, and recommended practices

- **EO-Critical Software**
 - Outlines targeted enhancements to existing C-SCRM guidance to support compliance with EO 14028
- **Software Cybersecurity for Producers and Users**
 - Guides federal acquirers towards SSDF v1.1 procurement activities that impact C-SCRM controls
 - Identifies risk-based scenarios in which enhanced attestation activities should be utilized
- **Software Verification**
 - Outlines targeted enhancements to existing C-SCRM guidance to support compliance with EO 14028
- **Cybersecurity Labeling for Consumers: Internet of Things (IoT) Devices and Software**
 - Provides traceability to latest web-based guidance



**Response
highlights |
Associated
web-based
guidance (II/II)**



Evolving standards, tools, and recommended practices

- **Software Bill of Materials (SBOM)**
 - Recaps current state of SBOM maturity and outlines practical enhancements that can be taken as this capability evolves
- **Enhanced Vendor Risk Assessments**
 - Describes enhancements to bolster vendor risk assessments for federal acquirers, especially within the context of Foreign Ownership, Control, or Influence (FOCI)
- **Open Source Software Controls**
 - Suggests a range of technical and procedural controls that federal acquirers can utilize to reduce open source software risks
- **Vulnerability Management Practices**
 - Reinforces the notion that effectively implementing and enhancing this capability is a requirement for yielding the benefits of EO concepts like Zero Trust and SBOM

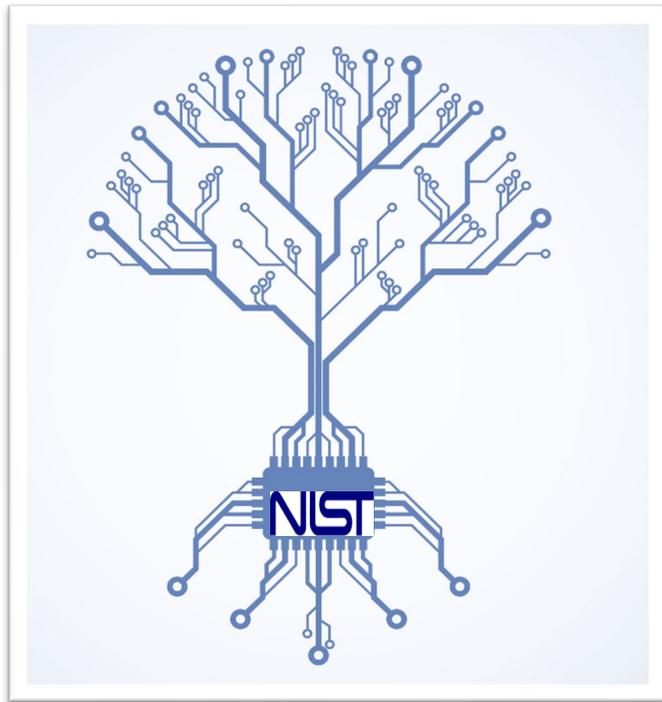
APPLY | Steps You Can Take

- REVIEW NIST guidance and initially ADOPT questions about the security of software your organization is developing or using.
- USE the four SSDF Practice Groups to organize communications about your existing software development or procurement.
 - “Prepare the organization,” “protect the software,” “produce well-secured software,” “respond to vulnerabilities.”
- Longer-term, INCORPORATE or REQUIRE that secure software development practices and cybersecurity supply chain measures be performed.
- ENGAGE by joining NIST at a workshop, submitting feedback on a publication, or joining as a collaborator at the NIST NCCoE.

What's Next?

- Update to NIST Cybersecurity Framework, considering supply chain issues and newer frameworks like the SSDF and the Privacy Framework.
- More on the National Initiative for Improving Cybersecurity in Supply Chains (NIICS), public-private partnership on supply chain.
- Leverage secure software efforts at the NCCoE, including to zero in on open-source software security challenges.
- Launch of Cybersecurity and Privacy Reference Tool (CPRT) to provide a consistent format for accessing the reference data of NIST cybersecurity publications like the SSDF.

Celebrating Our 50th Anniversary



The year 2022 marks **50 years** of NIST's cybersecurity research and the development of cybersecurity and privacy standards and guidance.

Our work has helped better secure the state of technology that exists today—while providing the platform for the secure technology development of tomorrow.

Celebrate with us all year long!

- Website: nist.gov/cybersecurity/50th-anniversary-cybersecurity-nist (events, resources, and blogs all in one place!)
- Follow @NISTcyber on Twitter and use #NISTCyber50th
- Subscribe for our GovDelivery updates (use URL above)

Stay in Touch!

NIST relies heavily on stakeholders. We hold public workshops, seek comments on draft documents, and welcome direct interactions.

www.nist.gov/cybersecurity



[Cybersecurity-
Privacy@nist.gov](mailto:Cybersecurity-Privacy@nist.gov)

