



**National Institute of
Standards and Technology**
U.S. Department of Commerce

Guidelines for Enhancing Software Supply Chain Security Under EO 14028

*Jon Boyens
Computer Security Division
IT Laboratory*

*NCCoE DevSecOPs Workshop
19 September 2022*

Sections of EO 14028

1. **Policy** – “... the prevention, detection, assessment, and remediation of cyber incidents is a top priority and essential to national and economic security. The Fed. Gov’t must lead by example...”
2. **Removing [Contractual] Barriers to Sharing Threat Information** – Incident Response Reporting
3. **Modernizing Fed. Gov’t Cybersecurity** – Move to...ZTA; Secure Cloud Services; Evaluate Data/MFA & Encryption
4. **Enhancing Software Supply Chain Security**
5. **Establishing a Cyber Safety Review Board.**
6. **Standardizing the Fed. Gov’t’s Playbook for Responding to Cybersecurity Vulnerabilities and Incidents**
7. **Improving Detection of Cybersecurity Vulnerabilities and Incidents on Fed. Gov’t Networks.**
8. **Improving Fed. Gov’t’s Investigative and Remediation Capabilities.**
9. **National Security Systems**
10. **Definitions**
11. **General Provisions**



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

EO-14028 Section 4 Guidance

Supply-Side

- Secure Software Development Framework (SSDF) (4e)
- Recommended Minimum Standards for Vendor or Developer Verification (Testing) of Software (4r)
- Attesting to Conformity with Secure Software Development Practices (4e)
- Software Bill of Materials minimum elements (4f) *NTIA*

Acquirer/Purchaser

- EO-Critical Software Definition (4g)
- Security Measures for EO-Critical Software (4i)
- Guidance on Software Cybersecurity for Producers and Purchasers – Guidance (4e)
- Guidance on Software Security in Supply Chains (4c/d)

EO-Critical Software

Any software that has, or has direct software dependencies upon, one or more components with at least one of these attributes:

- is designed to run with elevated **privilege** or manage **privileges**;
- has direct or **privileged access** to networking or computing resources;
- is designed to **control access** to data or operational technology;
- performs a function critical to **trust**; or,
- operates outside of normal **trust boundaries** with **privileged access**.

Security Measures for EO-Critical Software

Objectives

- 1: **Protect** software/platforms from unauthorized access and usage
- 2: **Protect** the confidentiality, integrity, and availability of data
- 3: **Identify** and maintain to protect from exploitation
- 4: Quickly **detect, respond to, and recover** from threats and incidents
- 5: **Strengthen** understanding and performance of humans' actions that foster security



Snapshot

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

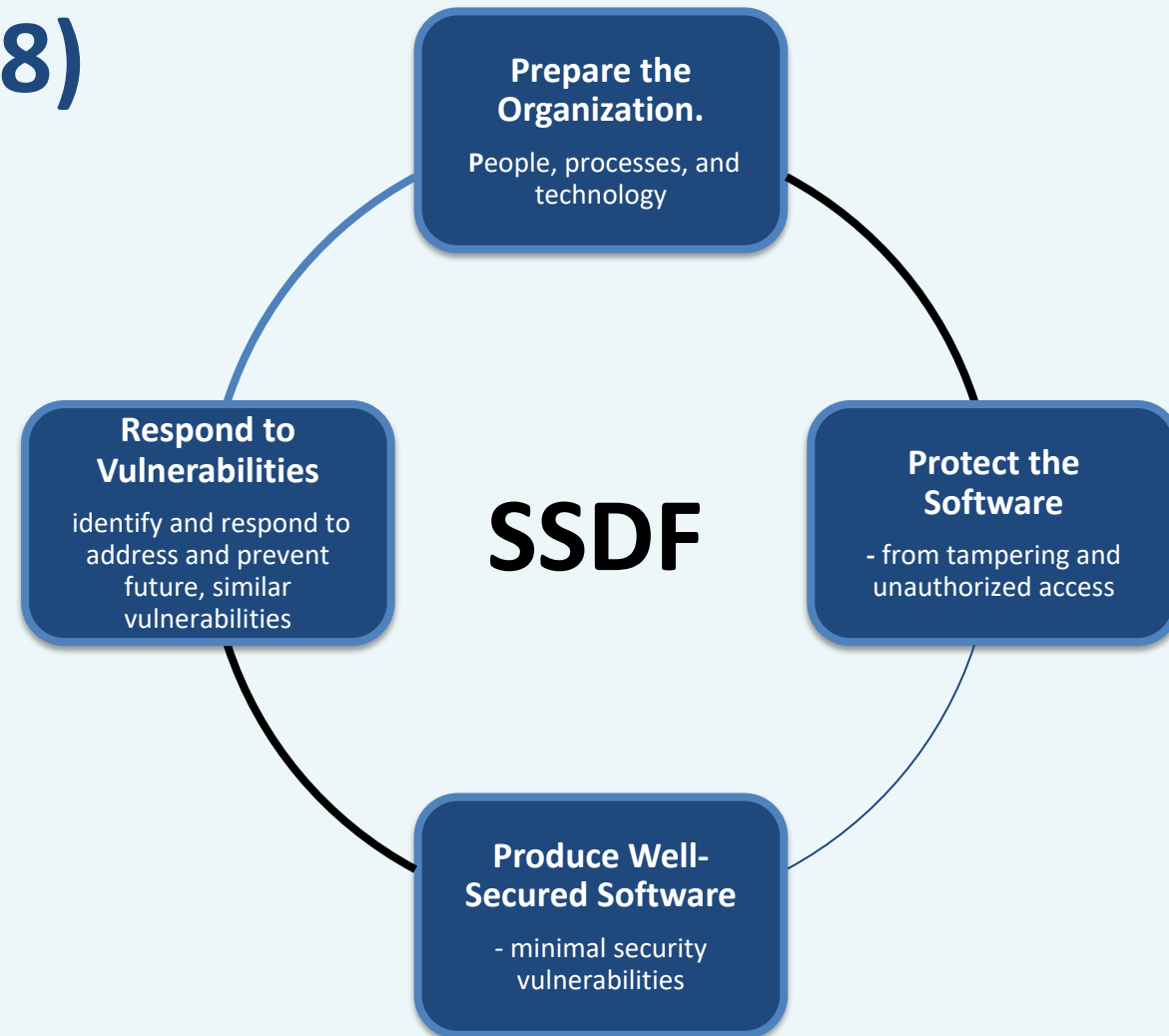
Security Measure 1.1: Use MFA that is verifier impersonation-resistant for all users and administrators of EO-critical software and EO-critical software platforms.

- 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

***OMB M-21-30: Protecting Critical Software Through Enhanced Security Measures**

Secure Software Development Framework version 1.1 (NIST SP 800-218)

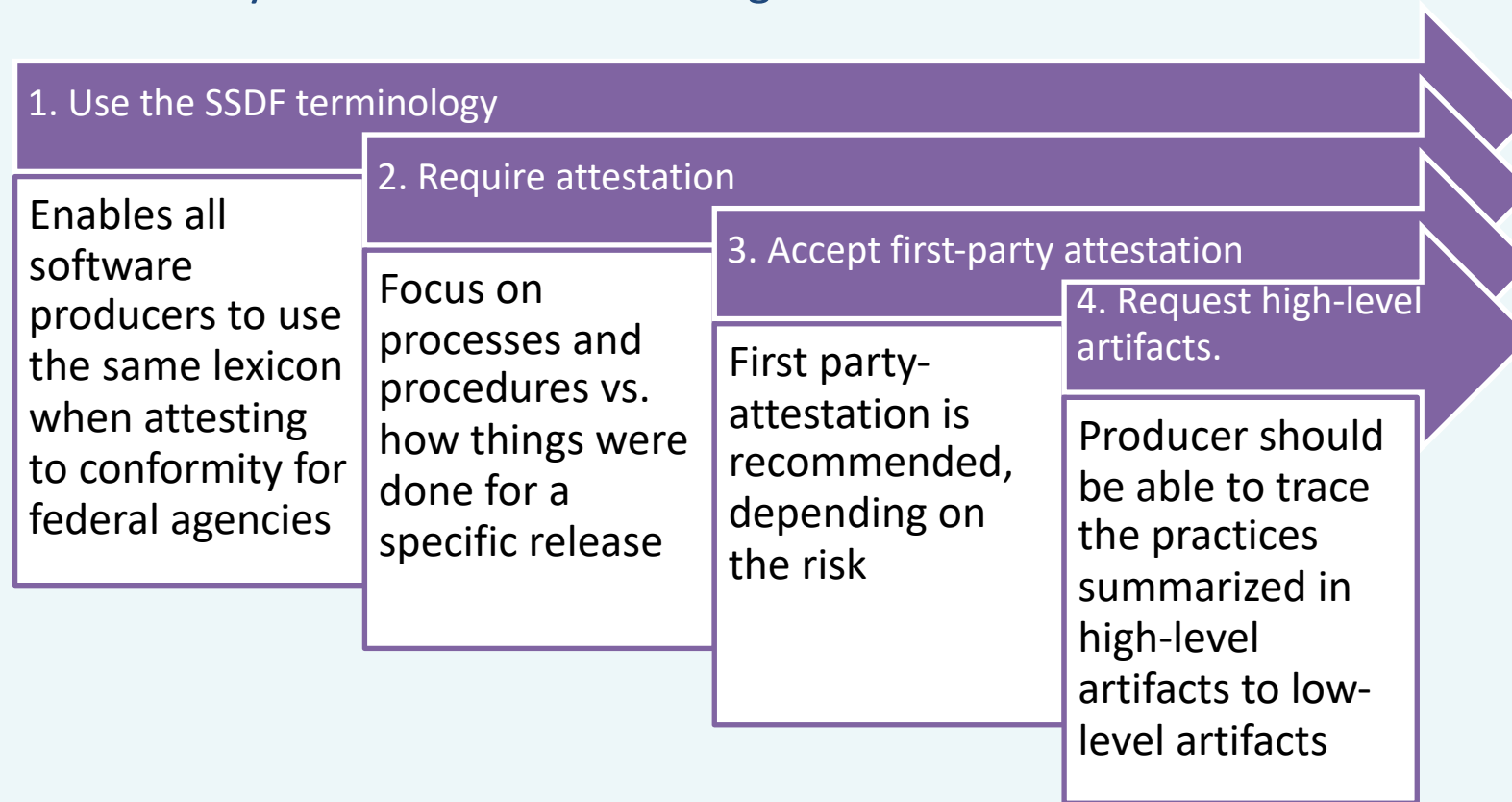
- Helps with adopting a risk management approach
 - document secure software development practices today
 - define future target practices.
- Provides a common lexicon & taxonomy
- Focus is on OUTCOMES not the “how”
- Leverages existing practices from established standards & guidance
- Broadly applicable to IT, IoT, OT



***OMB M-22-18:** *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*

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.



Software Verification

➤ 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

Appendix F: EO 14028 Sections 4(c)/(d) Response Guidance for Software Supply Chain Security

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

Available online to allow for update to guidance.



EO through the lens of 800-161

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

NIST's response to Sections 4c/d are housed in two primary locations

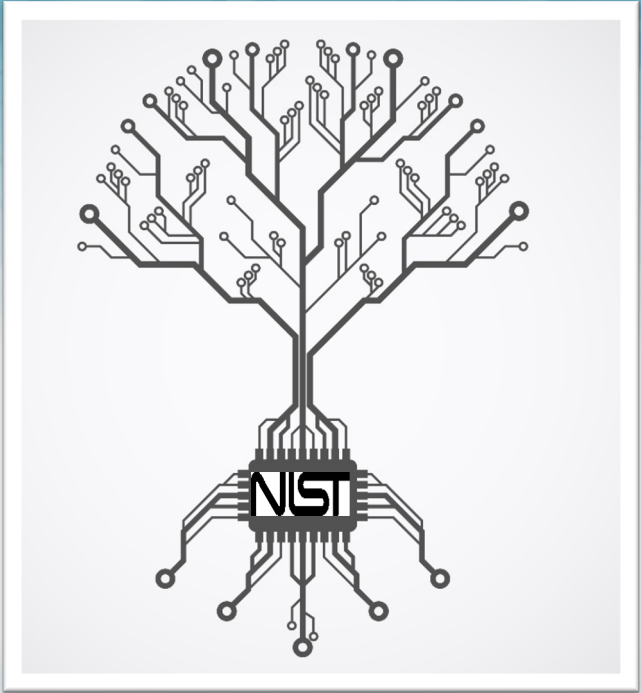


**SP 800-161 Rev. 1
Appendix F**



**Associated web-based
guidance**

*The web-based guidance is also available for
download as a PDF document*



Email: scrm-nist@nist.gov

Visit: <http://scrm.nist.gov>