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

Improving the Nation’s Cybersecurity: Progress and Next Steps in Carrying Out Executive Order 14028

Thursday, October 14, 2021 | 1:00 p.m. EDT

Agenda

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

1:00-1:05 p.m. EDT	**Introduction & Overview** Kevin Stine, Chief Cybersecurity Advisor, NIST
1:05-1:10 p.m. EDT	**Remarks from the National Security Council** Jeff Greene, Chief, Cyber Response & Policy, National Security Council
1:10-1:20 p.m. EDT	**Critical Software Definition, Security Measures, & Software Verification** Barbara Guttman, Leader, Software Quality Group, NIST
1:20-1:30 p.m. EDT	**(4c) Enhancing Software Supply Chain Security** Jon Boyens, Deputy Chief, Computer Security Division, NIST
1:30-1:40 p.m. EDT	**(4e) Secure Software Development Framework Update** Karen Scarfone, Scarfone Cybersecurity
1:40-1:50 p.m. EDT	**Labeling for Consumers: Internet of Things (IoT) Devices and Software** Warren Merkel, Chief, Standards Services, NIST
1:50-2:00 p.m. EDT	**Improving Cybersecurity in Supply Chains** Jon Boyens, Deputy Chief, Computer Security Division, NIST
2:00-2:15 p.m. EDT	**Facilitated Q&A**
2:15 p.m. EDT	**Conclusion**

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

Remarks from the National Security Council

Jeff Greene | NSC

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

Critical Software Definition & Security Measures

Software Verification

Barbara Guttman | NIST

Critical Software Definition & Security Measures

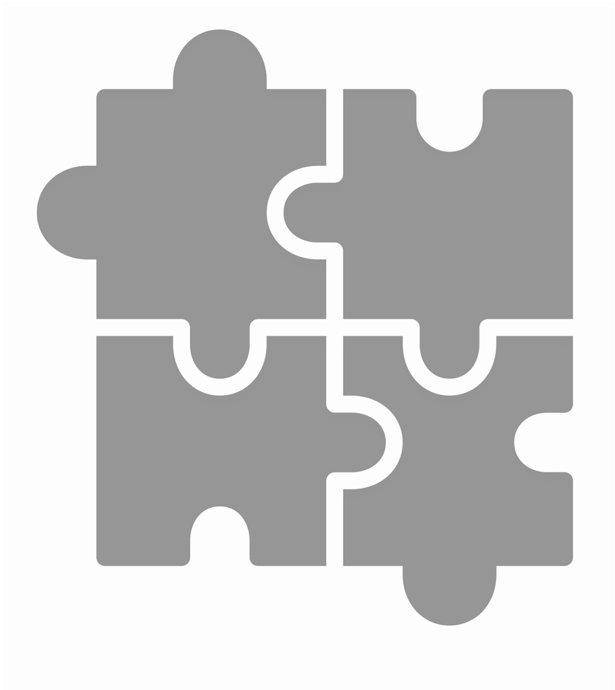
(g & i) … the Director of NIST…shall **publish a definition of the term "critical software**"(that) reflect(s) the level of privilege or access required to function, integration and dependencies with other software, direct access to networking and computing resources, performance of a function critical to trust, and potential for harm if compromised…and shall publish guidance outlining **security measures for critical software** as defined in subsection (g) of this section, including applying practices of least privilege, network segmentation, and proper configuration.

Definition

EO-critical software is defined as 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.

Strategy



- Given the complexity of the software, we recommended a phased approach.

- What this means is that we defined a subset of all possible software that could be considered critical.

.

Phases

- Initial phase: standalone, on-premises software that has security-critical functions or poses similar significant potentials for harm if compromised.
- Subsequent phases may address other categories of software such as: those that control access to data; cloud-based and hybrid software; software development tools such as development tools, testing software, code repository systems, integration software, packaging software, and deployment software; software components in boot-level firmware; and software components in operational technology (OT).

Initial List of Categories of EO-Critical Software

- ICAM
- Operating systems, hypervisors, container environments
- Web browsers
- Endpoint security
- Network control
- Network protection
- Network monitoring & configuration
- Operational monitoring & analysis
- Remote scanning
- Remote access & configuration management
- Backup/recovery & remote storage

Security Measures Strategy

- Specify key security measures for software, systems, and for people.
  - *Not exhaustive*

- Divided into objectives, measures, and links to resources.

Objectives

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

Software Verification

Section 4(r) - Within 60 days of the date of this order, the Secretary of Commerce acting through the Director of NIST, in consultation with the Secretary of Defense acting through the Director of the NSA, shall publish guidelines **recommending minimum standards for vendors' testing of their software source code**, including identifying recommended types of manual or automated testing (such as code review tools, static and dynamic analysis, software composition tools, and penetration testing).

Approach

- Minimum standards recommended for verification by software vendors or developers.
- No single verification standard can encompass all types of software testing, be specific and prescriptive, and present efficient and effective testing.
- Should be based on and in a Secure Software Development Process.

Structure

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

Techniques

- 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

4(c) Enhancing Software Supply Chain Security

Jon Boyens | NIST

EO 14028 Section 4(c)

Section 4 (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.*

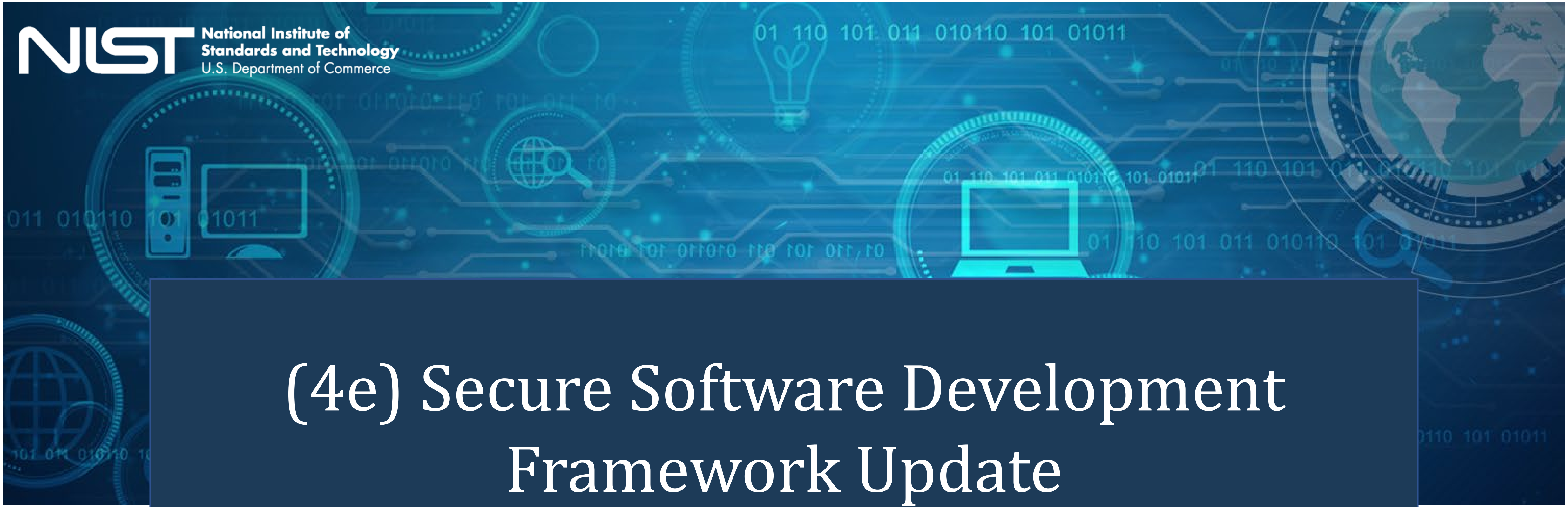
Approach

- Use existing industry standards, tools, and recommended practices sourced from the main body of draft SP 800-161 Revision 1.
- Use previous guidance published by NIST as a result of the EO, including:
  - **Definition of Critical Software** Under Executive Order (EO) 14028; June 25, 2021
  - **Security Measures for "EO-Critical Software"** Use Under Executive Order (EO) 14028; July 9, 2021
  - **Guidelines on Minimum Standards for Developer Verification** of Software; July 2021
- New standards, tools, and recommended practices sourced from over 150 position papers stemming from Section 4 (b) workshop in June 2021.
- Other related software supply chain-related work in the EO.
- Foundational, Sustaining, Enhancing.

EO 14028 Section 4(c), Continued

- Security Measures for EO-Critical Software
  - Recommend flowing down controls to suppliers
- Guidelines on Minimum Standards for Developer Verification
  - Developed a chart where verification techniques can be used as part of various C-SCRM controls
- NOT IN THIS DRAFT: Section 4 (e) Secure Software Development Framework (TBD)
- Cybersecurity Labeling for Consumers: IoT Devices and Software
  - FISMA is applicable to IoT so applicable security measures should be already in place
  - NISTIR 8259 *Recommendations for IoT Device Manufacturers: Foundational Activities* as well as NISTIR 8259A *Core Device Cybersecurity Capability Baseline*
  - CISA's *Internet of Things Acquisition Guidance*
  - *NOT IN THIS DRAFT: Draft SP 800-213 IoT Device Cybersecurity Guidance for the Federal Government* (TBD)

- Emerging software supply chain concepts (Foundational, Sustaining, Enhancing)
  - Software Bill of Materials (SBOM)
  - Enhanced Vendor Risk Assessments
  - Open Source Software Controls
  - Vulnerability Management Practices
- Existing Industry Standards, Tools, and Recommended Practices


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

(4e) Secure Software Development Framework Update

Karen Scarfone | Scarfone Cybersecurity

(4e) directs NIST to "issue guidance identifying practices that enhance the security of the software supply chain," to include…

- (i) securing software development environments.
- (iii) maintaining trusted source code supply chains.
- (iv) checking for known and potential vulnerabilities and remediating them.
- (vi) maintaining provenance of software code or components, and controls on software components, tools, and services for software development processes.
- (vii) providing an SBOM for each product.
- (viii) participating in a vulnerability disclosure program.

SSDF Publication Basics

Initial SSDF white paper finalized in April 2020

Provides a common language to describe fundamental, sound secure software development practices

Set of 19 practices; one or more tasks per practice, and implementation examples and references for each task

Already addressed much of what (4e) specified and could easily be expanded to include the rest

Had been planning on revising the SSDF to address the latest threats against software development, increase preparation for secure software use, and update the references

Asked for public input on (4b) & (4e)

- (4b) directed NIST to “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 (e).”
- Held virtual workshop on June 2-3, 2021 and received over 150 position papers.
- Received and reviewed all suggestions for new and updated practices, tasks, implementation examples, and references.

Draft SP 800-218, SSDF Version 1.1 Out for Public Comment

- Released on September 30th; comment period ends **November 5th.**
- Added references based on public input, including IEC 62443 (ICS/OT), OWASP MASVS (mobile), and OWASP SCVS and CNCF SSCP (supply chain).
- Added practice PO.5, Implement and Maintain Secure Environments for Software Development.
- Created Appendix A to map EO clauses to the SSDF practices and tasks that help address each clause.

4(e) also directs NIST to “issue guidance identifying practices that enhance the security of the software supply chain,” to include…

- (ii) providing artifacts that demonstrate conformance to (i) processes.
- (v) providing artifacts of tool and process execution for (iii) and (iv) and making available summary information publicly available.
- (ix) attesting to conformity with secure software development practices.
- (x) ensuring and attesting to the integrity and provenance of open-source software used within a product.

Help Us Improve the SSDF & Address the EO

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

https://csrc.nist.gov/projects/ssdf
&
ssdf@nist.gov

- Submit your comments on Draft SP 800-218 by **November 5th**.
- If your organization has produced a set of secure software development practices and you want to map them to the SSDF, please email us so we can introduce you to the National Online Informative References (OLIR) Program. You can contribute your mapping to our collection of informative references.
- We want your thoughts about what types of artifacts can be captured, documented, and shared publicly as byproducts of implementing the SSDF practices. Are there examples you can share?

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

Labeling for Consumers: IoT Devices & Software

Warren Merkel | NIST

EO Directives & Milestones

NIST, in coordination with representatives of other agencies…shall initiate pilot programs informed by existing consumer product labeling programs to educate the public on the security capabilities of internet-of-Things (IoT) devices and software development practices and shall consider ways to incentivize manufacturers and developers to participate in these programs.

Within 270 days (February 6, 2022), NIST, in coordination with the Federal Trade Commission (FTC) & other agencies shall:

✓ Identify **IoT cybersecurity criteria for a consumer labeling program**

- Consider whether such a consumer labeling program may be operated in conjunction with or modeled after any similar existing government programs
    - The criteria shall:
    - Reflect increasingly comprehensive levels of testing and assessment that a product may have undergone.
    - Use or be compatible with existing labeling schemes that manufacturers use to inform consumers about the security of their products.

✓ Identify **secure software development practices or criteria for a consumer software labeling program**

- Consider whether such a consumer software labeling program may be operated in conjunction with or modeled after any similar existing government programs.
    - The criteria shall reflect a baseline level of secure practices, and if practicable, shall reflect increasingly comprehensive levels of testing and assessment that a product may have undergone.
- Identify, modify, or develop a recommended label or, if practicable, a tiered software security rating system.

NIST Approach

- Open, transparent, collaborative, inclusive.
- NIST will **identify key elements of labeling programs in terms of minimum requirements and desirable attributes – rather than establishing its own programs.**
- Labeling should:
  - Encourage innovation in manufacturers' IoT security efforts, leaving room for changes in technologies and the security landscape.
  - Be practical and not be burdensome to manufacturers and distributors.
  - Factor in usability as a key consideration.
  - Build on national and international experience.
  - Allow for diversity of approaches and solutions across industries, verticals, and use cases – so long as they are deemed useful and effective for consumers.

Activities to Date

- Consultation with public and private sector stakeholders
- Landscape review of existing consumer IoT labeling and CA initiatives
  - National and international policy initiatives
  - Standards
  - Existing IoT device labeling schemes
- Call for papers on consumer software labeling
- Published white paper with DRAFT Baseline Security Criteria for Consumer IoT Devices
  - Open for comments through October 17, 2021
- Public workshop September 14-15, 2021

What’s Next

- Review comments on DRAFT Baseline Security Criteria for Consumer IoT Devices
- Publish DRAFT criteria for consumer software labeling by end of October 2021
- Publish final criteria for consumer IoT devices and consumer software by February 2022
- Consult with the private sector and relevant agencies to assess the effectiveness of the programs
- Publish final report by May 12, 2022

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

Improving Cybersecurity in Supply Chains

Jon Boyens | NIST

Facilitated Q&A

Thanks for joining us!