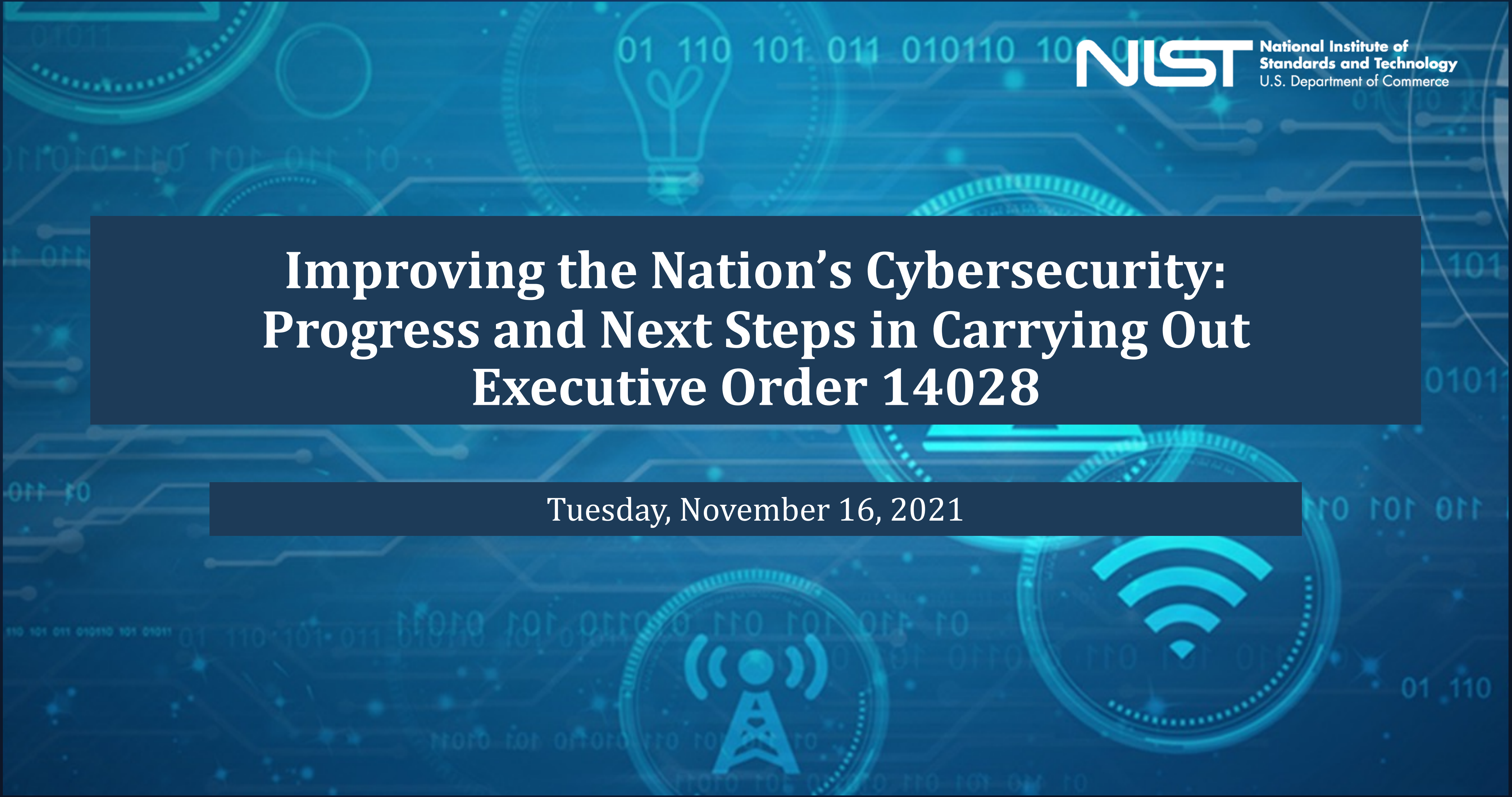
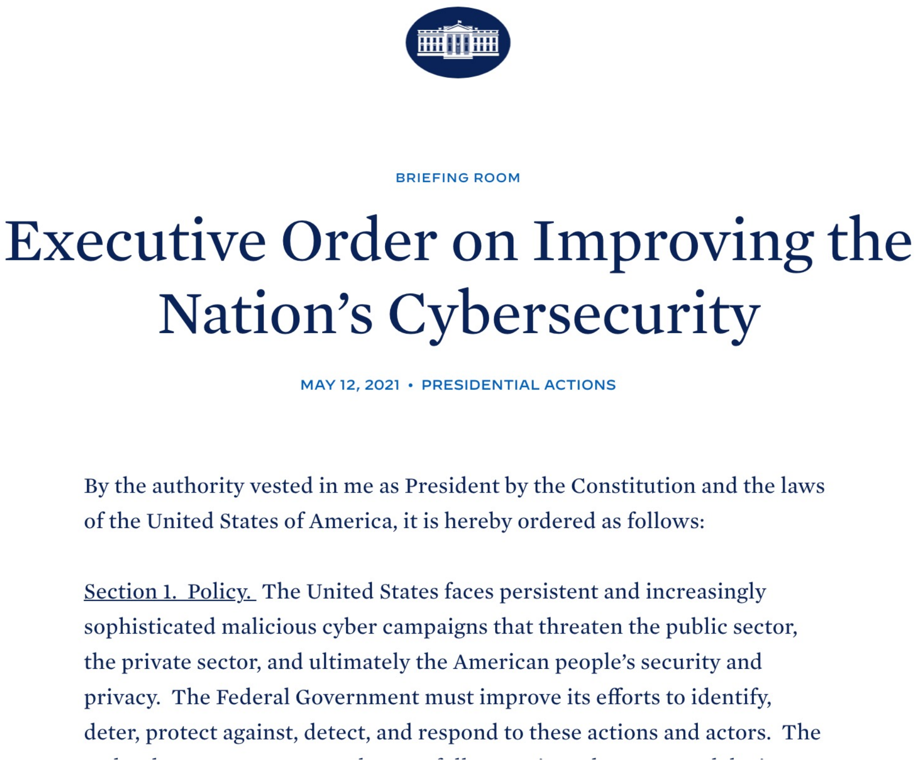


NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

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

Tuesday, November 16, 2021

Executive Order 14028



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

Section 2 – Removing Barriers to Sharing Threat Information

Section 3 – Modernizing Federal Government Cybersecurity

Section 4 – Enhancing Software Supply Chain Security

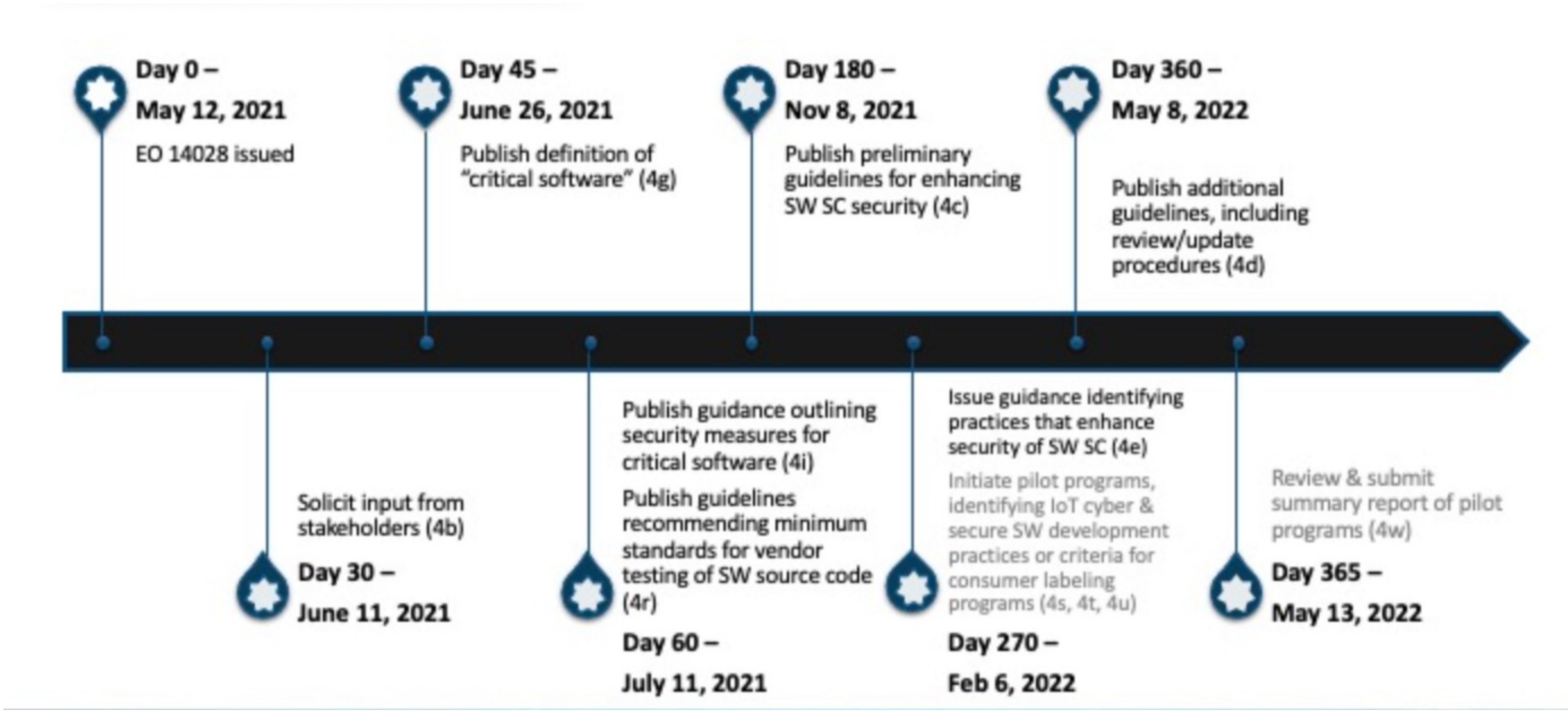
Section 5 – Establish a Cyber Safety Review Board

Section 6 – Standardizing the Fed Gov's Playbook for Responding to Cybersecurity Vulns and Incidents

Section 7 – Improving Detection of Cybersecurity Vulns and Incidents on Fed Gov Networks

Section 8 – Improving the Fed Gov's Investigative and Remediation Capabilities

NIST's Responsibilities



Day 0 –

May 12, 2021

EO 14028 issued

Solicit input from stakeholders (4b)

Day 30 –

June 11, 2021

Day 45 –

June 26, 2021

Publish definition of "critical software" (4g)

Publish guidance outlining security measures for critical software (4i)

Publish guidelines recommending minimum standards for vendor testing of SW source code (4r)

Day 60 –

July 11, 2021

Day 180 –

Nov 8, 2021

Publish preliminary guidelines for enhancing SW SC security (4c)

Issue guidance identifying practices that enhance security of SW SC (4e)

Initiate pilot programs, identifying IoT cyber & secure SW development practices or criteria for consumer labeling programs (4s, 4t, 4u)

Day 270 –

Feb 6, 2022

Day 360 –

May 8, 2022

Publish additional guidelines, including review/update procedures (4d)

Review & submit summary report of pilot programs (4w)

Day 365 –

May 13, 2022

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

Defining Critical Software and Security Measures

Software Verification

Critical Software Definition & Security Measures

(4g) directs NIST to "publish a definition of... critical software"
and
(4i) directs NIST to "publish guidance outlining security measures for critical software..."

The definition must address...

- 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...

The guidance must include 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 tec**hnology;
- Performs a function **critical to trust**; or
- Operates **outside of normal trust boundaries** with privileged access.

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

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

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

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

Taxonomy

- **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.

Objective 1: Protect EO-critical software and EO-critical software platforms from unauthorized access and usage.	
SM 1.1: Use multi-factor authentication that is verifier impersonation-resistant for all users and administrators of EO-critical software and EO-critical software platforms. (See FAQ #7.)	•**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

Software Verification

(4r) directs NIST to "publish guidelines recommending minimum standards for vendors' testing of their software source code, …"

- 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.

Techniques

- **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

- 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

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

4(c) Enhancing Software Supply Chain Security

EO 14028 Section 4(c)

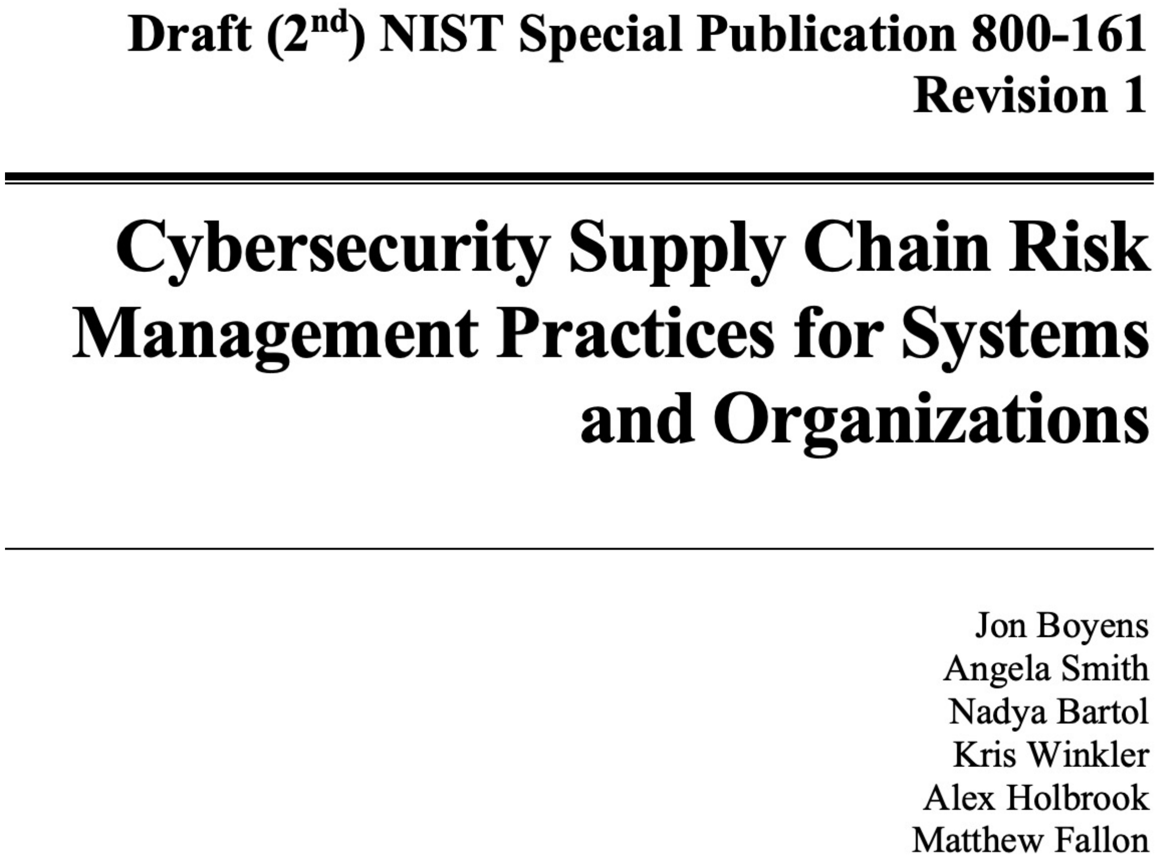
(4c) directs NIST to “publish preliminary guidelines… for enhancing software supply chain security…”

- 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 in response to the EO
- New standards, tools, and recommended practices sourced from over 150 position papers stemming from Section 4 (b) workshop in June 2021.
- Foundational, Sustaining, and Enhancing Capabilities

EO 14028 Section 4(c), Continued

- EO Critical Software Definition
- Software Verification
- Cybersecurity Labeling for Consumers (IoT and Software)

- 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

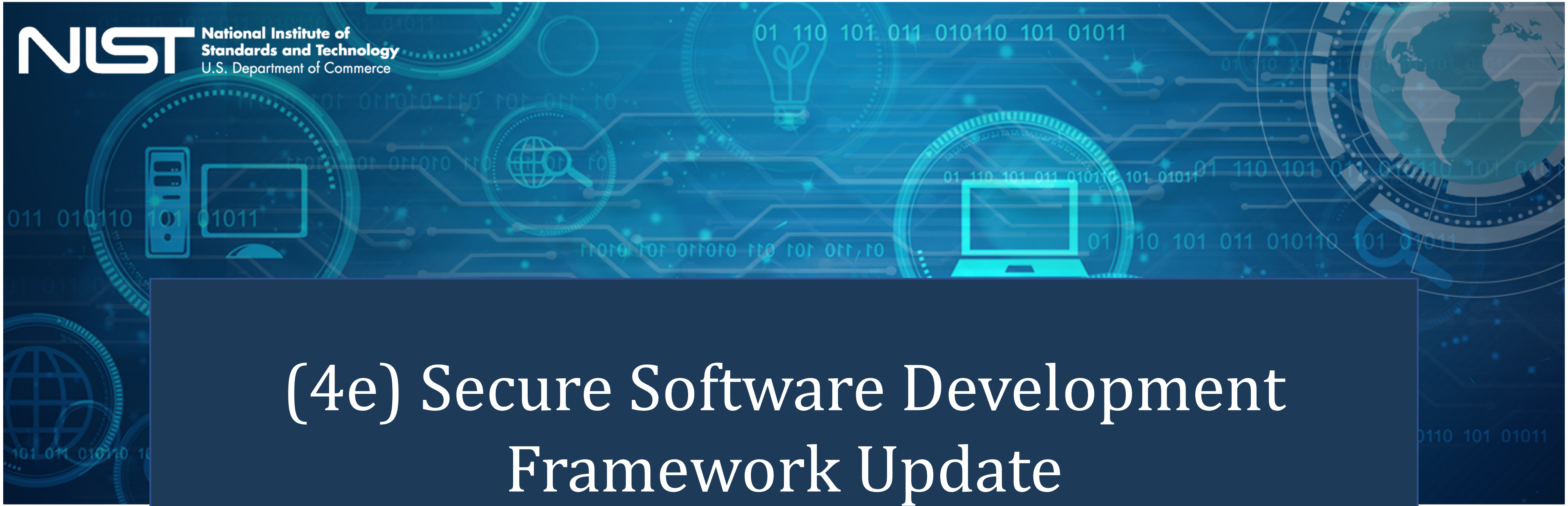


Draft (2nd) NIST Special Publication 800-161
Revision 1

Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations

Jon Boyens
Angela Smith
Nadya Bartol
Kris Winkler
Alex Holbrook
Matthew Fallon

Comments Due 12/3/21: https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/draft



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

(4e) Secure Software Development Framework Update

(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

Draft SP 800-218, SSDF Version 1.1

- Released on September 30th; comment period ended **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.

Labeling for Consumers: IoT Devices & Software

EO Directives & Milestones

4(s/t/u) directs NIST to … 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 ...

✓ 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

✓ 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.

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

- Consulted with public and private sector stakeholders
- Conducted a landscape review of existing consumer IoT labeling and conformity assessment initiatives
  - National and international policy initiatives
  - Standards
  - Existing IoT device labeling schemes
- Issued 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
- Hosted a public workshop September 14-15, 2021
- Published draft criteria for consumer software labeling on Nov 1; comments due Dec 16.

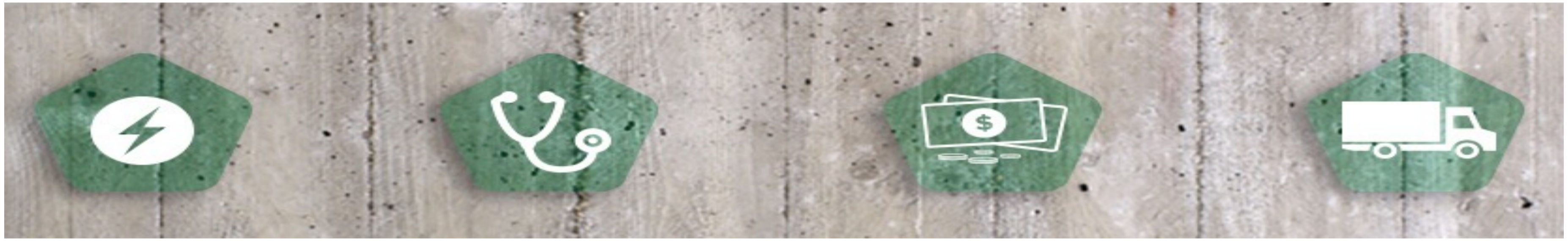
What’s Next on Labeling

- Review comments on DRAFT security criteria for consumer IoT devices and consumer software
- 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

Accelerate adoption of secure technologies: collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs

Current NCCoE Projects

- Crypto Agility: Considerations for Migrating to Post-Quantum Crypto Algorithms
- Implementing a Zero Trust Architecture
- 5G Cybersecurity
- Supply Chain Assurance: Validating the Integrity of Computing Devices
- Ransomware Risk Management
- Securing the Industrial Internet of Things: Cybersecurity for Distributed Energy Resources
- Cybersecurity for Genomics Data
- Trusted IoT Device Network-Layer Onboarding and Lifecycle Management



Engage with Us!

Get the latest updates and track progress at https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity

Send input and questions to swsupplychain-eo@nist.gov

Work with the NCCoE: https://nccoe.nist.gov

For more opportunities to engage with NIST on Cybersecurity and Privacy, please visit https://www.nist.gov/cybersecurity/cybersecurity-privacy-stakeholder-engagement

Thank You