NIST CYBERSECURITY & PRIVACY PROGRAM

EXECUTIVE ORDER ON IMPROVING THE NATION'S CYBERSECURITY

The President's Executive Order on Improving the Nation's Cybersecurity (EO 14028), issued May 12, 2021, charges multiple agencies – including the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) – with enhancing the security of the software supply chain.

Section 4 of the Executive Order (EO) directs the Secretary of Commerce, through NIST, to consult with federal agencies, the private sector, academia, and other stakeholders and to identify or develop standards, tools, best practices, and other guidelines to enhance software supply chain security. The resulting standards and guidelines will be used by other agencies to govern the federal government's procurement of software.

NIST also is assigned responsibilities related to cybersecurity labeling of Internet of Things (IoT) products and consumer software. NIST has a longstanding program focused on managing risks to the cyber supply chain, software quality and security, and security development and engineering resources – across research, standards and guidelines, and transition to practice. Resources published by NIST and others served as a starting point for assignments under the EO. **NIST has completed all assignments under the EO.**

GUIDELINES

The guidelines are to address: critical software, secure software development lifecycle, security measures for the federal government, and requirements for testing software. They are to include:

- Criteria to evaluate software security,
- Criteria to evaluate the security practices of the developers and suppliers themselves, and
- Innovative tools or methods to demonstrate conformance with secure practices.

After consulting with multiple agencies:

- ✓ By **June 26, 2021**, NIST defined "critical software."
- ✓ By **July 11, 2021**, NIST published guidance outlining security measures for critical software as well as guidelines recommending minimum standards for vendors' testing of their software source code.
- ✓ By **November 8, 2021**, NIST published preliminary guidelines, based on stakeholder input and existing documents for enhancing software supply chain security.
- ✓ By **February 6, 2022**, NIST issued guidance that identified practices that enhanced software supply chain security, including standards, procedures, and criteria.
- ✓ By **May 7, 2022**, NIST published additional guidelines, including procedures for periodically reviewing and updating guidelines.

WORKSHOPS AND POSITION PAPERS

To ensure robust stakeholder participation in developing standards and guidelines to be produced, NIST has held multiple workshops to share details about its plans to develop software-related standards and guidelines called for by the EO and to receive and discuss information and ideas about the approach and content that NIST should consider. Agendas have been based in part on position papers and comments submitted to NIST by organizations and individuals. NIST has published those papers and lists of resources to improve software security.

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

CYBERSECURITY LABELING FOR CONSUMERS

The EO also directs NIST to initiate two cybersecurity labeling initiatives related to:

- The Internet of Things (IoT) and
- Consumer software.

These efforts are aimed at informing consumers about the security of their products. NIST worked closely with other government agencies and private and public sector organizations and individuals in carrying out these initiatives. That included holding multiple workshops, soliciting position papers, and seeking comments on draft criteria for IoT products and software labeling.

NIST identified key elements of labeling programs in terms of minimum requirements and desirable attributes. Rather than establishing its own programs, NIST specified desired outcomes, allowing providers and customers to choose best solutions for their device sand environments. One size may not fit all, and multiple solutions might be offered by label providers.

NIST submitted the report to the Assistant to the President for National Security Affairs (APNSA), as directed in the EO. It is available HERE.

NIST CYBERSECURITY FUNDAMENTALS

- ✓ **OPEN AND TRANSPARENT: NIST's processes bring together stakeholders in an open forum.**
- ✓ **COLLABORATIVE: NIST provides a space for government agencies, businesses, and academic institutions to collaborate.**
- ✓ **PRACTICAL: NIST helps develop practical example solutions to address real-world challenges.**
- ✓ **FORWARD-THINKING: NIST looks to the future and anticipates challenges that lie ahead.**

More information about this work is available on a dedicated website.

Information about NIST's broader portfolio of work in cybersecurity and privacy can be found here.

Questions should be directed to: swsupplychain-eo@list.nist.gov.

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