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 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 will serve as a starting point for assignments under the EO.

GUIDELINES

The guidelines will 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 is to define "critical software."
- ✓ By July 11, 2021, NIST is to publish 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 is to publish preliminary guidelines, based on stakeholder input and existing documents for enhancing software supply chain security.
- By **February 6, 2022**, NIST will issue guidance that identifies practices that enhance software supply chain security, including standards, procedures, and criteria.
- By **May 8, 2022**, NIST will publish additional guidelines, including procedures for periodically reviewing and updating guidelines.

WORKSHOP AND POSITION PAPERS

To ensure robust stakeholder participation in developing standards and guidelines to be produced, NIST held a workshop June 2-3, 2021, 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.

The agenda was based on position papers submitted to NIST by organizations and individuals. NIST has published those papers and lists of resources to improve software security.

CYBERSECURITY LABELING FOR CONSUMERS

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

- the Internet of Things (IoT) and
- secure software development practices.

These efforts are aimed at informing consumers about the security of their products. NIST will work closely with other government agencies and private and public sector organizations and individuals in carrying out these initiatives.

That includes a workshop in September. In advance of that session, NIST will solicit position papers on software labeling and publish for comment a draft white paper on the landscape of current IoT labeling schemes.

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