




May 26, 2021

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Cisco would like to thank the National Institute of Standards and Technology (NIST) for the opportunity to file these comments in response to the [Workshop and Call for Position Papers on Standards and Guidelines to Enhance Software Supply Chain Security](#). President Biden's [Executive Order 14028](#), aimed at improving the security of federal agencies, is both ambitious and necessary. It creates several efforts that have been needed for many years and several more where the need has just become evident. Cisco is committed to maintaining strong protections for our customers, partners, products, and company. We strive to earn trust by being trustworthy, transparent, and accountable. These goals are embodied in [Cisco's Trust Principles](#), which map well to the software-related standards and guidelines NIST is required to develop pursuant to the Executive order. We look forward to working with NIST and other agencies on implementing these efforts and would be happy to offer relevant experts to speak to any of the topics outlined below:

We respectfully submit the attached paper on Cisco's initial position, and requests for clarity around the five areas addressed.

DocuSigned by:

04A598590121432...
Eric Wenger
Senior Director, Technology Policy
erwenger@cisco.com | 202-354-2948

DocuSigned by:

CC7D83CF392347B...
Jeff Schutt
Security and Trust Architect
jfschut@cisco.com | 408-526-7989

Cisco Systems
170 West Tasman Dr
San Jose, CA 95134 USA

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706

Phone: 408 526-4000
Fax: 408 526-4100
www.cisco.com



May 26, 2021

- 1. *Criteria for designating "critical software."* Functional criteria should include, but not be limited to, level of privilege or access required to function, integration, dependencies, direct access to networking and computing resources, performance of a function critical to trust, and potential for harm if compromised. See EO Section 4(g).**

Least privilege is a common control and best practice employed to minimize exposure and limit access to software. Cisco suggests that it would be useful for NIST to flesh out whether and how security concepts such as "least privileged access" and the creation of dependencies should relate to a decision to designate "critical software." One approach might be to designate as "critical software" software that is necessary to provide critical security functions such as encryption, decryption, identification, authentication, segmentation, and integrity verification?

We believe a risk-based approach to designating "critical software" is needed. Such an approach should take into account the performance of functions critical to trust within a software package, within a product, and within an operational system. Aspects of the product, service, solution, and system deployment patterns should also be considered, including considerations like on-premise infrastructures' ability to maintain functionality in air-gapped environments, and dependencies on cloud technologies.

- 2. *Initial list of secure software development lifecycle standards, best practices, and other guidelines acceptable for the development of software for purchase by the federal government. This list of standards shall include criteria and required information for attestation of conformity by developers and suppliers. See EO Section 4(e)(i, ii, ix, and x).***

Cisco Secure Development Lifecycle (SDL) ensures that Cisco's entire portfolio of products, services, and solutions are designed using industry-leading practices and technology to ensure their resiliency and trustworthiness. From planning to development, [Cisco SDL](#) includes threat modelling and analysis to determine security requirements and builds appropriate protections into its design and coding. It is a repeatable and measurable process that all employees, contractors, consultants, temporary, and other workers at Cisco and its subsidiaries ("Cisco workers") that are involved with product, system, or solution development are required to follow.

Cisco SDL includes:

- Secure coding standards and safe coding libraries
- The registration of commercial and open-source code
- Plans for handling security alerts
- Gap analysis against Cisco's internal security baseline requirements
- Testing for protocol robustness, vulnerabilities, and application security

- 3. *Guidelines outlining security measures that shall be applied to the federal government's use of critical software, including but not limited to, least privilege, network segmentation, and proper configuration. See E.O. Section 4(I).***

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706

Phone: 408 526-4000
Fax: 408 526-4100
www.cisco.com



May 26, 2021

There are a range of industry standards that address security measures, controls and best practices. Cisco believes that a baseline of security measures should be identified that mitigate the most common and egregious mistakes, weaknesses, and risks seen in federal government systems. Wherever possible, identified security measures should reference existing industry-led, consensus-based standards. Given the ever-changing nature of the threat landscape, NIST guidelines should articulate risk-based measures necessary to secure against known types of threats and deployment patterns. The proposed measures should be flexible enough to address evolutions in technology and in the behavior of threat-actors. Additionally, NIST should provide a path to adoption that prioritizes higher-impact measures over others dependent upon the deployment pattern and threat landscape. Finally, the approach should be processed base, enabling greater maturity at managing risk to the target state more effectively over time.

4. *Initial minimum requirements for testing software source code including defining types of manual or automated testing (such as code reviewed tools, static and dynamic analysis, software composition tools, and penetration testing), their recommended uses, best practices, and setting realistic expectations for security benefits. See EO Sections 4(e)(iv and v) and 4(r).*

There are numerous efforts specifically focused on enabling software providers to reduce risk by testing software source code. Cisco encourages NIST to provide guidance on the types of testing, recommended uses, best practices, and security benefits. At the same time, care must be given to decisions about who should perform such testing and where it should be conducted. Cisco would encourage NIST to focus will be on self-assessment with artifacts capable of being independently validated rather than some system of government inspection of commercial source code, which would clearly set an unacceptably negative security precedent throughout the world.

5. *Guidelines for software integrity chains and provenance. See EO Sections 4(e)(ii, vi, and viii).*

We encourage the continued development, support and adoption of existing consensus-based standards and specifications that enable software integrity chains and provenance at scale. Cisco is in support of initiatives by the NTIA to enable [software transparency](#) and demonstrate the value of software bills of materials (SBOM). SBOMs are a foundational element that will provide more transparency throughout the [value chain](#), and are necessary in providing a solution to address the risks called out in the Executive Order. Implementations of metadata describing software integrity chain and provenance must be small, machine-readable and cryptographically verified if they wish to scale to solve for the landscape of today's technology infrastructure. These artifacts should be able to be exchanged between the various tools throughout the software supply chain. We desire NIST to include support for the two leading SBOM formats: SPDX and CycloneDX. We encourage NIST to evaluate existing work and standards that can articulate the linkage between an SBOM and the vulnerability disposition of each listed components, anticipating future vulnerability searches to be based on SBOM data. Cisco also encourages NIST to publish guidelines that enable implementation of repeatable and reproducible builds.

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706

Phone: 408 526-4000
Fax: 408 526-4100
www.cisco.com