

Notice and Request for Information about Evaluating and Improving Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management

Cisco's response to the U.S. Department of Commerce
National Institute of Standards and Technology (NIST)
Request for Information

May 3, 2022

May 3, 2022

Cisco Systems would like to thank the National Institute of Standards and Technology (NIST) for the opportunity to provide this response to the Notice and Request for Information about Evaluating and Improving Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management (RFI).¹ Cisco recognizes the value of standards-based, process-oriented best practices for cybersecurity supply chain risk management and appreciates the work NIST does to advance this goal.

Cisco recommends the following considerations as NIST develops updates for the Cybersecurity Framework (CSF) and Cybersecurity Supply Chain Risk Management leveraging feedback received in response to the RFI:

- First, Cisco believes supply chain risk management should focus more attention on the **end-to-end security of the lifecycle of key products—leveraging trustworthy technologies and integrity verification** to validate secure supply chains. Trustworthy technology examples for NIST to consider include: digital software image signing; hardware-anchored secure boot; establishing a chain of trust for critical software; Trust Anchor Modules; and runtime defenses. Security features at the operating system, application, and data layers can then be built upon a foundation of trust anchored to hardware.
- Second, Cisco recommends that **third-party risk management should be more integrated** with the CSF as core business practices, rather than solely relying on secondary frameworks. Trends in the attack landscape necessitate increased vigilance surrounding all interactions with third parties. This integration should include, at a minimum: 1) controls recommending that vendors provide lists of authorized and continuously reevaluated resellers; and 2) controls guiding best practices for data governance and security guidelines for data shared with or stored by third parties. Cisco believes NIST Special Publication (SP) 800-53 Rev. 5 identified the right Supply Chain Risk Management (SCRM) controls for vendors to map to.² By way of example, Cisco has successfully mapped our Value Chain Security Architecture, Trustworthy Technologies, Policies, Procedures and Teams to each relevant control, as illustrated below. The CSF should move towards incorporating similar SCRM controls, most notably SR-4-3, Identify as Genuine and Not Altered, SR-9, Tamper Resistance and Detection, and SR-11, Component Authenticity. These integrations will advance the goal of seeding greater adoption across government, critical infrastructure, and enterprises.

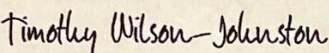
¹ <https://www.federalregister.gov/documents/2022/02/22/2022-03642/evaluating-and-improving-nist-cybersecurity-resources-the-cybersecurity-framework-and-cybersecurity>

² <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>

- Lastly, to assist adherence to Executive Order 14028,³ NIST should provide guidance on **how the CSF should be applied alongside the Secure Software Development Framework (SSDF)**. One way to do this could be to map the SSDF Practices and Tasks as Informative References in the CSF.

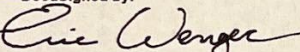
Cisco looks forward to the results of this enhancement to cybersecurity resources and the benefits it will bring across organizations. We thank you again for your consideration.

Sincerely yours,

DocuSigned by:

D80BAF3306534D6...

Timothy Wilson-Johnston, Value Chain Security Leader,

@cisco.com


DocuSigned by:

04A598590121432...

Eric Wenger, Senior Director, Technology Policy

@cisco.com

³ <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>

Cisco Systems NIST 800-53 Rev.5 SCRM Mapping

 NIST 800-53 SCRM Mapping		Master Security Specification	Cisco Secure Development Lifecycle	Supply Chain Security Team	InfoSec	Acquisition & Integration Team	Secure Boot	Trust Anchor Module	Approved Vendor List	Supply Chain Resiliency Team	Quality Assurance	PSIRT	Brand Protection Team
Control	Name	Value Chain Security Architecture				Trustworthy Technology	Cisco Policies, Procedures, and Teams						
SR-1	Policy and Procedures	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓
SR-2	Supply Chain Risk Management Plan	✓	✓	✓	✓					✓			✓
SR-2 (1)	Establish SCRM Team			✓	✓					✓			✓
SR-3	Supply Chain Controls and Processes	✓		✓	✓		✓	✓	✓	✓	✓		
SR-3-1	Diverse Supply Base			✓	✓				✓	✓			
SR-3-2	Limitation of Harm			✓	✓				✓	✓			✓
SR-3-3	Sub-Tier Flow Down	✓		✓	✓				✓	✓			✓
SR-4	Provenance		✓	✓	✓		✓	✓				✓	
SR-4-1	Identity	✓		✓	✓								✓
SR-4-2	Track and Trace	✓		✓	✓								✓
SR-4-3	Validate as Genuine and Not Altered	✓	✓	✓	✓			✓			✓		✓
SR-4-4	Supply Chain Integrity - Pedigree	✓		✓	✓		✓	✓					✓
SR-5	Acquisition Strategies, Tools, and Methods			✓	✓	✓			✓				
SR-5-1	Adequate Supply			✓	✓	✓			✓	✓			
SR-5-2	Assessments Prior to Selection, Acceptance, Modification, or Update		✓	✓	✓								✓
SR-6	Supplier Assessments and Reviews	✓		✓	✓				✓				
SR-6-1	Testing and Analysis	✓	✓	✓	✓								
SR-7	Supply Chain Operations Security	✓		✓	✓				✓				✓
SR-8	Notification Agreements	✓		✓	✓					✓			
SR-9	Tamper Resistance and Detection	✓		✓	✓		✓	✓					✓
SR-9-1	Multiple Stages of System Development Lifecycle	✓	✓	✓	✓		✓	✓					
SR-10	Inspection of Systems and Components	✓		✓	✓								
SR-11	Component Authenticity	✓	✓	✓	✓		✓	✓				✓	✓
SR-11-1	Anti-Counterfeit Training	✓		✓	✓								✓
SR-11-2	Config Control for Component Service and Repair	✓		✓	✓								✓
SR-11-3	Anti-Counterfeit Scanning	✓	✓	✓	✓		✓	✓			✓		✓
SR-12	Component Disposal	✓		✓	✓								✓