PUBLIC SUBMISSION

As of: 4/25/22 12:47 PM
Received: April 23, 2022
Status: Pending_Post
Tracking No. l2b-z199-0t2r
Comments Due: April 25, 2022
Submission Type: Web

Docket: NIST-2022-0001
Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management

Comment On: NIST-2022-0001-0001
RFI-2022-03642

Document: NIST-2022-0001-DRAFT-0033
Comment on FR Doc # N/A

Submitter Information

Email: [redacted]
Organization: Hewlett Packard Enterprise

General Comment

"NIST Cybersecurity RFI" comments attached, from Chris Hibbard and other Cybersecurity professionals Hewlett Packard Enterprise

Attachments

RFI_Feedback Improving NIST Cybersecurity Resources_HPE_PSO-B HPE

All comments are inline in green highlight.

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

Published Document

This document has been published in the *Federal Register*. Use the PDF linked in the document sidebar for the official electronic format.

AGENCY:

National Institute of Standards and Technology (NIST), Commerce.

ACTION:

Notice; request for information.

SUMMARY:

The National Institute of Standards and Technology (NIST) is seeking information to assist in evaluating and improving its cybersecurity resources, including the “Framework for Improving Critical Infrastructure Cybersecurity” (the “NIST Cybersecurity Framework,” “CSF” or “Framework”) and a variety of existing and potential standards, guidelines, and other information, including those relating to improving cybersecurity in supply chains. NIST is considering updating the NIST Cybersecurity Framework to account for the changing landscape of cybersecurity risks, technologies, and resources. In addition, NIST recently announced it would launch the National Initiative for Improving Cybersecurity in Supply Chains (NIICS) to address cybersecurity risks in supply chains. This wide-ranging public-private partnership will focus on identifying tools and guidance for technology developers and providers, as well as performance-oriented guidance for those acquiring such technology. To inform the direction of the NIICS, including how it might be aligned and integrated with the Cybersecurity Framework, NIST is requesting information that will support the identification and prioritization of supply chain-related cybersecurity needs across sectors. Responses to this RFI will inform a possible revision of the Cybersecurity Framework as well as the NIICS initiative.

DATES:

Comments in response to this notice must be received by April 25, 2022. Submissions received after that date may not be considered.

Comments may be submitted by any of the following methods:

Electronic submission: Submit electronic public comments via the Federal e-Rulemaking Portal.

1. Go to *www.regulations.gov* and enter NIST-2022-0001 in the search field,

2. Click the “Comment Now!” icon, complete the required fields, and

3. Enter or attach your comments.

Electronic submissions may also be sent as an attachment to *CSF-SCRM-RFI@nist.gov* and may be in any of the following unlocked formats: HTML; ASCII; Word; RTF; or PDF. Please submit comments only and include your name, organization's name (if any), and cite “NIST Cybersecurity RFI” in all correspondence. Comments containing references, studies, research, and other empirical data that are not widely published should include copies of the referenced materials. Please do not submit additional materials.

Comments received by the deadline may be posted at *www.regulations.gov* and *https://www.nist.gov/cyberframework*. All submissions, including attachments and other supporting materials, may become part of the public record and may be subject to public disclosure. NIST reserves the right to publish relevant comments publicly, unedited and in their entirety. Personal information, such as account numbers or Social Security numbers, or names of other individuals, should not be included. Do not submit confidential business information, or otherwise sensitive or protected information. Comments that contain profanity, vulgarity, threats, or other inappropriate language or content will not be considered.

FOR FURTHER INFORMATION CONTACT:

For questions about this RFI contact: *CSF-SCRM-RFI@nist.gov* or Katherine MacFarland, National Institute of Standards and Technology, 100 Bureau Drive, Stop 2000, Gaithersburg, MD 20899; (301) 975-3359. Direct media inquiries to NIST's Office of Public Affairs at (301) 975-2762. Users of telecommunication devices for the deaf, or a text telephone, may call the Federal Relay Service, toll free at 1-800-877-8339.

Accessible Format: NIST will make the RFI available in alternate formats, such as Braille or large print, upon request by persons with disabilities.

SUPPLEMENTARY INFORMATION:

The NIST Cybersecurity Framework consists of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to reduce cybersecurity risks. It is used widely by private and public sector organizations in and outside of the United States and has been translated into multiple languages, speaking to its success as a common resource.

The Cybersecurity Framework was last updated in April 2018. Much has changed in the cybersecurity landscape in terms of threats, capabilities, technologies, education and workforce, and the availability of resources to help organizations to better manage cybersecurity risk. That includes an increased awareness of and emphasis on cybersecurity risks in supply chains, including a decision to launch NIICS. With those changes in mind, NIST seeks to build on its efforts to cultivate trust by advancing cybersecurity and privacy standards and guidelines, technology, measurements, and practices by requesting information about the use, adequacy, and timeliness of the Cybersecurity Framework and the degree to which other NIST resources are used in conjunction with or instead of the Framework. Further, to inform the direction of the NIICS, including how it might be aligned and integrated with the Cybersecurity Framework, NIST is requesting information that will support the identification and prioritization of supply chain-related cybersecurity needs across sectors.

Following is a non-exhaustive list of possible topics that may be addressed in any comments. Comments may address topics in the following list, or any other topic believed to have implications for the improvement of the NIST Cybersecurity Framework or NIST's cybersecurity guidance regarding supply chains. NIST will consider all relevant comments in the development of the revised Framework and guidance regarding supply chains.

Use of the NIST Cybersecurity Framework

1. The usefulness of the NIST Cybersecurity Framework for aiding organizations in organizing cybersecurity efforts via the five functions in the Framework and actively managing risks using those five functions.

The NIST Cybersecurity Framework seems to rely on references. It does not have examples within. Further information on standards for providing data, to assist in defining maturity levels (i.e., provide examples of something at Adaptive maturity level for each area without being too restrictive as to create a difficulty—a minimum standard) would be helpful.

Also, the Framework would be much easier to use if it included examples in all Functions that could be used as a sample for developing Profiles.

2. Current benefits of using the NIST Cybersecurity Framework. Are communications improved within and between organizations and entities (*e.g.*, supply chain partners, customers, or insurers)? Does the Framework allow for better assessment of risks, more effective management of risks, and/or increase the number of potential ways to manage risks? What might be relevant metrics for improvements to cybersecurity as a result of implementation of the Framework?

The framework helps deploy a standard process to different organizations and suppliers and helps us communicate with suppliers and partners by offering a consistent methodology and common means of documentation.

However, the framework is lacking a base profile that could be used to develop a Target Profile. This would support organizations implementing the Framework and improving the capability to identify risks.

We could use something similar to NISTIR-8183 (Manufacturing), but for Software.

Metrics for Package Naming problem:

- Naming Collisions across Vendors

- Mismatches (public repositories refer to the same package with 2 different names)
- % False positives in packages reported by Tools provided to discovered FOSS

Package Trust score metrics:

- Time to fix
- Frequency of releases with security fixes
- Security Impact rating of Package's potential risk (measures degree high trust scores are needed)

Also, the industry could use some Metrics for measuring a Vendor's compliance against a target profile. Finally, have you considered implementing metrics from the CHAOSS or GRIMOIRE projects for purposes of assessing the health of a given component from a supply chain perspective?

3. Challenges that may prevent organizations from using the NIST Cybersecurity Framework or using it more easily or extensively (*e.g.*, resource considerations, information sharing restrictions, organizational factors, workforce gaps, or complexity).

Workforce gaps and training gaps will be pan-industry. Guidelines or recommendations regarding the # of security professionals needed per product/ developer would be helpful. Also, better automation in tools helps workforce gaps (somewhat).

The NIST Framework documentation could use more examples and guidelines. Organizations need to invest in additional training and resources to create a Profile to ensure compliance.
The NIST Framework documentation could use more examples and guidelines.

NIST could provide training materials, or guidelines for training vendors to provide training Suppliers who wish to comply.

Individual companies/organizations should not be trying to create their own metrics separately, NIST should provide guidance so that companies/organizations can appropriately baseline and tool vendors (e.g., Revenera, Synopsys, Syft, etc.) ("Tool Vendors") can assist in compliance.

A tool to measure compliance with EO14028 would be well used and very helpful. Tool Vendors provide pieces of the puzzle but without a strong ecosystem in place to enable organizations to quickly scale assessment of components for an EO SBOM, the requirements of this system will hamper innovation, time-to-market and consistency.

4. Any features of the NIST Cybersecurity Framework that should be changed, added, or removed. These might include additions or modifications of: Functions, Categories, or Subcategories; Tiers; Profile Templates; references to standards, frameworks, models, and guidelines; guidance on how to use the Cybersecurity Framework; or references to critical infrastructure versus the Framework's broader use.

NIST should provide templates with examples of controls including guidance/ presentations /training on how Profile creation and use of Tiers.

If NIST adds new controls for SBOMs, they need to be added to the Cybersecurity Framework Crosswalk (see, https://www.nist.gov/privacy-framework/resource-repository/browse/crosswalks/cybersecurity-framework-crosswalk)("Crosswalk Document"), so the controls are cross referenced for multiple standards to ensure interoperability across the industry . Clear deadlines and a grace period for implementation will also be necessary features of any successful implementation of such requirements.

5. Impact to the usability and backward compatibility of the NIST Cybersecurity Framework if the structure of the framework such as Functions, Categories, Subcategories, etc. is modified or changed.

Backwards compatibility with any new structures must be considered especially in the context of automated tooling that may not have the flexibility to accommodate such changes.

6. Additional ways in which NIST could improve the Cybersecurity Framework, or make it more useful.

Naming conventions of Open Source packages must be established. Who will police this? The industry needs a standard for an automated gathering of package names from all publicly available vendors…with a stress on a unique name for each package that is reliable and repeatable (designed to reduce naming collisions and naming mismatches). The Common Platform Enumeration (CPE - https://csrc.nist.gov/projects/security-content-automation-protocol/specifications/cpe) Naming system is not acceptable to use for EO-compliant SBOMs because the # of packages listed is too small, and it does not use Vendor-supplied names as required in NTIAs Minimum Data Elements document.

We suggest making a similar document to NISTIR 8183 (for Manufacturing) but specific to SBOMs and the Software Supply Chain in general.

NIST should also add recommendations concerning Ransomware in the Cybersecurity Framework.

Relationship of the NIST Cybersecurity Framework to Other Risk Management Resources

7. Suggestions for improving alignment or integration of the Cybersecurity Framework with other NIST risk management resources. As part of the response, please indicate benefits and challenges of using these resources alone or in conjunction with the Cybersecurity Framework. These resources include:

- Risk management resources such as the NIST Risk Management Framework, the NIST Privacy Framework, and Integrating Cybersecurity and Enterprise Risk Management (NISTIR 8286).

  The industry needs better alignment between CSF and CSCRM Process (SP 800-161 Rev. 1). Today, SP 800-161 provides a level of valuable details and guidance that if the CSF implemented, it would be much more useful.

- Trustworthy technology resources such as the NIST Secure Software Development Framework, the NIST Internet of Things (IoT) Cybersecurity Capabilities Baseline, and the Guide to Industrial Control System Cybersecurity.

  The industry needs a standard for Vendors to publicly provide data on fixes provided for vulnerabilities. This will allow for metrics to quantify how reliable packages are. The metric should include how quickly vulnerabilities are fixed, and how large the pool of active contributors is to assess the overall health of a project. NIST should consider integrating the metrics tracked by the Linux Foundation's CHAOSS project (https://chaoss.community/) to achieve this.

- Workforce management resources such as the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity.

  No comment.

8. Use of non-NIST frameworks or approaches in conjunction with the NIST Cybersecurity Framework. Are there commonalities or conflicts between the NIST framework and other voluntary, consensus resources? Are there commonalities or conflicts between the NIST framework and cybersecurity-related mandates or resources from government agencies? Are there ways to improve alignment or integration of the NIST framework with other frameworks, such as international approaches like the ISO/IEC 27000-series, including ISO/IEC TS 27110?

There is not enough commonality between NIST and other data resources such as GitHub and other public repositories. Today they use different names (with no clear way to match them up) and NIST CPE makes to attempt to create a comprehensive list of all available open source, so there is a large number of packages with no official names.

The industry needs a better standard naming scheme that encompasses all others, something with which Tool Vendors can claim compatibility.

NIST needs to integrate the Crosswalk document with all new controls so entities can find the compatibility between standards. The more standards they map to, the more useful they become.

9. There are numerous examples of international adaptations of the Cybersecurity Framework by other countries. The continued use of international standards for cybersecurity, with a focus on interoperability, security, usability, and resilience can promote innovation and competitiveness while enabling organizations to more easily and effectively integrate new technologies and services. Given this importance, what steps should NIST consider to ensure any update increases international use of the Cybersecurity Framework?

We would like to see more documentation on commonality with similar Supply Chain Security and Cybersecurity efforts in the EU (such as the Cyber Resilience Act), / UK (such as UK NIS Regulations), and others. This has been lacking in past standards.

10. References that should be considered for inclusion within NIST's Online Informative References Program. This program is an effort to define standardized relationships between NIST and industry resources and elements of documents, products, and services and various NIST documents such as the NIST Cybersecurity Framework, NIST Privacy Framework, Security and Privacy Controls for Information Systems and Organizations (NIST Special Publication 800-53), NIST Secure Software Development Framework, and the NIST Internet of Things (IoT) Cybersecurity Capabilities Baseline.

Cybersecurity Supply Chain Risk Management

11. National Initiative for Improving Cybersecurity in Supply Chains (NIICS). What are the greatest challenges related to the cybersecurity aspects of supply chain risk management that the NIICS could address? How can NIST build on its current work on supply chain security, including software security work stemming from E.O. 14028, to increase trust and assurance in technology products, devices, and services?

Provide or align with standardized naming scheme [with unique identifiers], provide incentives for industry scanning SW to use it. (Include all Packages, all Vendors)

[NIST] standard should Provide trust ratings for Vendors and packages, based on public vulnerability documented fix rate data, and contributor activity, in a standard format (beginning with public repositories of packages such as GitHub).

12. Approaches, tools, standards, guidelines, or other resources necessary for managing cybersecurity-related risks in supply chains. NIST welcomes input on such resources in narrowly defined areas (*e.g.* pieces of hardware or software assurance or assured services, or specific to only one or two sectors) that may be useful to utilize more broadly; potential low risk, high reward resources that could be facilitated across diverse disciplines, sectors, or stakeholders; as well as large-scale and extremely difficult areas.

Tools available today are inconsistent and not compatible. NIST needs to have clearly defined standards that Tool Vendors can clearly state they support. The industry needs a standard that is as well-used as CVE that does what CPE fails to do. This full package list might come from self-registered components (if all Vendors chose to participate), or it could be auto-updated from common [public] package repositories [GitHub and others] which could have an additional advantage in pulling fix histories to create trustability scores for packages and Vendors.

13. Are there gaps observed in existing cybersecurity supply chain risk management guidance and resources, including how they apply to information and communications technology, operational technology, IoT, and industrial IoT? In addition, do NIST software and supply chain guidance and resources appropriately address cybersecurity challenges associated with open-source software? Are there additional approaches, tools, standards, guidelines, or other resources that NIST should consider to achieve greater assurance throughout the software supply chain, including for open-source software?

Same as above: The entire industry needs a standard for unique and reliable naming (free from collisions and duplicates/ mismatches) for all Packages from all Vendors.

Ransomware guidance is a big gap, NIST should integrate NISTIR 8374 (Ransomware). Given the increase of ransomware, this is a critical gap to fill.

14. Integration of Framework and Cybersecurity Supply Chain Risk Management Guidance. Whether and how cybersecurity supply chain risk management considerations might be further integrated into an updated NIST Cybersecurity Framework—or whether and how a new and separate framework focused on cybersecurity supply chain risk management might be valuable and more appropriately be developed by NIST.

Expand on Risk Management section of CSF. Existing 3 sections are not adequate, needs to more adequately cover Remediation/ Response and Trust Scale [of Open Source Packages and Vendors]. In 2018 NIST withdrew their Guide to Selection of IT Security Products, but did not replace it. Should be specifically replaced, NIST still has references to this expired doc.

A separate document for an SBOM Profile (similar to existing Manufacturing NISTIR8183) would be very useful and help more Orgs comply.

Alicia Chambers,

NIST Executive Secretariat.

[FR Doc. 2022-03642 Filed 2-18-22; 8:45 am]

BILLING CODE 3510-13-P