Operational Technology Cybersecurity Coalition

April 25, 2022

National Institute of Standards and Technology
Applied Cybersecurity Division
Cybersecurity Framework
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899
Submitted via email to CSF-SCRM-RFI@nist.gov

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

NIST ACD CSF Team:

The Operational Technology Cybersecurity Coalition (OT Cyber Coalition) appreciates the opportunity to submit feedback to the teams at the National Institute of Standards and Technology (NIST) working on potential updates to the Cybersecurity Framework (CSF).

The OT Cyber Coalition is a diverse group of leading cybersecurity vendors, founded by Claroty, Forescout, Honeywell, Nozomi Networks, and Tenable. Representing the entire OT lifecycle, the OT Cyber Coalition believes that the strongest, most effective approach to securing our nation's critical infrastructure is one that is open, vendor-neutral, and allows for diverse solutions and information sharing without compromising cybersecurity defenses.

As a foundational cybersecurity standard, the impact of the existing guidance and any future guidance is monumental. In order to help better inform the community of stakeholders that will rely on the NIST CSF, we offer the following feedback that incorporates perspectives gained from every sector and phase of the cybersecurity lifecycle. While we have responded to specific questions, the ultimate goal of our feedback is to promote a standards-based approach that allows for vendor- and technology-neutral solutions to be adopted by anyone, anywhere, and in any sector.

Specific Responses

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.

Despite the fact the NIST CSF has not been updated since 2018, it remains among the most important cybersecurity standards, both nationally and internationally. From an OT perspective, it has been very useful in outlining how and why the five functions are important to addressing the cybersecurity lifecycle for OT and ICS assets. Most importantly, especially for those sectors that lack targeted guidance, it provides an industry-accepted baseline for what should provide at least a basic level of protection and a technology- and vendor-neutral pool of solutions providers.

One area of improvement worth considering would be outlining how each of the Functions interacts with and impacts one another. For example, an action focusing on the Detect Function will be reliant on certain outputs from the Identify Function and may trigger responses or activities related to the Protect, Response, and Recovery Functions. Showing these links, even if through examples, will help reinforce the necessity to address all Core Functions in a robust and mature cybersecurity strategy.

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?

Among the key advantages of the NIST CSF has been the development of a foundational common taxonomy that can be used not only for more effective communications but also to more clearly assess and address risks by reducing the potential for miscommunication or misunderstandings. This also allows for the development of metrics that provide stakeholders the ability to understand adoption levels. Examples of metrics that can be objectively measured to determine implementation levels include the number of known versus unknown assets in a network or the number of users who are using MFA versus the number who are not.

These raw numbers are, of course, not enough on their own. Metrics that measure the amount of time it takes to improve implementation should be recommended, and where

feasible, developed and shared. Understanding how long it takes to turn an unidentified asset into an identified one or bringing the organization to complete compliance with multi-factor authentication (MFA) practices provides valuable insight that could signify most significant organizational issues. These metrics also provide important insight into gaps such as a lack of the appropriate tools or training, how these gaps impact implementation, as well as where and how those gaps may result in organization-specific risks and the potential resulting impact during an actual incident.

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).

Many of the challenges cited are real, significant, and often lead to either partial or improper implementation of the NIST CSF. Among the root causes of these challenges and others that organizations face is the use of proprietary systems. Closed systems or ecosystems harm general threat intelligence by restricting information sharing, limiting the pool of potential tools or talent that will support an organization's cybersecurity posture, and ultimately reducing the ability to automate away many of the issues associated with resource constraints, scale, and complexity. For example, the use of technology that fails to leverage STIX/TAXII as a method to ensure open sharing of information can impact the ability of an organization to appropriately monitor its threat environment.

Whether through accompanying guidance or one or more Categories and Subcategories, encouraging organizations to identify and understand the impact of using proprietary versus standards-based tools within their overall enterprise architecture is an essential component of any long-term strategic planning associated with achieving and maintaining a certain level of cybersecurity maturity. This is particularly true in OT environments and with critical infrastructure, where an incident that cannot be detected, responded to, mitigated, and recovered from in a timely manner can result in severe economic damage, such as exhibited with food and fuel operators, or severe injury and death, as has already occurred with incidents taking place in hospitals and medical environments. Using an open or standards-based approach throughout the entire cybersecurity lifecycle will provide all organizations with access to the widest possible pool of approaches and assistance to improve implementation and address incidents.

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.

The current structure of the NIST CSF has proven to be accessible and digestible by a broad enough swath of industry and the workforce that any changes should be incremental and intentional. For example, the Functions, Categories, and Subcategories have been mapped to and built upon by other standards focused on specific sectors or use cases. Similarly, the Tiers and references provide additional, relevant, and important guidance that is necessary to achieve greater maturity and focus on those specific activities that will help that organization achieve its Target Profile(s). While all could use updates to reflect new lessons learned and best practices, the general structure and format has achieved a commendable level of familiarity among the appropriate stakeholders.

When it comes to the Profile Templates and the references to critical infrastructure versus broader applicability, there is value in providing either guidance or recommended approaches to allow organizations to prioritize how they address gaps in general implementation. Beyond providing additional informative content, such guidance, when developed using information gleaned from public and private sector experiences, will help address other root causes associated with those challenges in implementation identified in the previous question. Being able to better budget for the work associated with implementation and having additional data points when deciding the technology choices necessary will provide value to all users, whether critical infrastructure or not.

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.

The more significant the change, the more significant the impact will be on the usability and backward compatibility of the NIST CSF. Tools, techniques, talent, and the trainings used to spread familiarity with all of them have been developed with the existing structure in mind. While nothing is perfect and there are updates to content and objectives that can be made based on the latest developments in cybersecurity generally, some of which have been identified in this response already, the value of the structure to promote understanding has been proven. This can be seen by the significant number of private sector participants that have voluntarily adopted the framework and the number of other countries that have adapted it, including Israel, Italy, and Japan. Piloting any potential proposed changes with a broad swath of stakeholders

and providing ample opportunity to provide input and feedback will be essential to mitigate the negative impact and maximize the positive impact of any such changes.

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

Ultimately, harmonization between the NIST CSF and other resources should be the goal. From taxonomy and terminology to controls and compliance, ensuring that the people and products developed to support the cybersecurity maturity of organizations that have adopted the NIST CSF, as has been mentioned throughout this response, is critical. Cybersecurity is a team sport and making sure the team can make valid assumptions about how certain actions will play out in the middle of an active incident will be critical. For example, as emerging concepts like the software bill of materials (SBOM) or hardware bill of materials (HBOM) may not be finalized until after an update to the NIST CSF has been published, how they align with Core Functions and relevant Categories or Subcategories should not be left up to interpretation.

This is particularly true when it comes to alignment with the NICE Workforce Framework for Cybersecurity and public sector job descriptions, some of which are used to inform private sector job descriptions. While there will always be corollary subjects that must be understood to have full comprehension of most emerging components that will ultimately be incorporated into current and future frameworks, the NIST CSF has proven that it can and most likely should serve as the baseline upon which the resources mentioned should be developed upon. This will give current and future practitioners the necessary ability to quickly implement new concepts like SBOM and HBOM.

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?

Where feasible, harmonization should be a priority. Especially for those who are following those non-NIST frameworks, having a better understanding of where the NIST CSF and those other resources align would provide important value to those who have yet to adopt the NIST CSF. For those who wish to comply with numerous standards, such as NIST SP 800-53 and the ISO/IEC standards mentioned, having guidance that outlines how prioritizing adoption of the NIST CSF will ultimately enable an organization to quickly comply with the requirements of all three if not more relevant industry or sector-specific standards. Where feasible, reciprocity in terms of implementation of a particular NIST CSF Category or Subcategory should be recommended or established.

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?

Two particular steps could prove impactful: greater participation in international standards-setting bodies like the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) through the American National Standards Institute (ANSI) and a focus on translating actionable guidance, such as that released by the National Cybersecurity Center of Excellence (NCCoE).

Greater participation in the standards-setting bodies would not only provide an opportunity to improve harmonization between the NIST CSF and non-NIST resources, but it would also expose the NIST CSF to the international audiences that have the necessary influence on their nation's public and private sector organizations that would benefit from the adoption of the NIST CSF. While NIST has a long and important history

in participating with ISO and IEC[1] as well as ANSI and other relevant organizations, being targeted and specific in ensuring alignment between other proposed standards and the NIST CSF will be an important component of any broader engagement strategy.

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?

While individual efforts towards addressing cybersecurity supply chain risk management (C-SCRM) continue to advance, there would be great value in unifying these efforts, much like the SECURE Technology Act and the Federal Acquisition Supply Chain Council, among other efforts, have recognized. Clarity about what to use and how to secure an organization's supply chain, whether in terms of the software and hardware it relies on or the contractors and subcontractors that support them, is currently lacking. A framework for supply chain risk management should be incorporated into the NIST CSF itself to address this gap.

Additionally, providing insight into how CSF best practices and C-SCRM assessments can be applied to existing inventories would be useful. Beyond providing greater visibility into risks that may exist within an organization's supply chains to the lowest tier subcontractor feasible, understanding the broader environment within which that organization operates will help further efforts to support a zero trust architecture (ZTA).

[1] *See, e.g.*, DeVaux, C. (2000), A Review of U.S. Participation in the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.IR.6492 (February 1, 2000; Accessed April 9, 2022)

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?

Greater assistance could be provided to the Sector Risk Management Agencies (SRMAs) to adopt the NIST CSF as part of their sector-specific guidance. Beyond the usual enhancements that come from providing additional resources, subject matter expertise, and authorities to implement the framework, the previously mentioned recommendation to develop metrics that measure the impact of activities on overall adoption and to establish mappings that provide what and how to achieve reciprocity between the CSF and non-CSF activities would help address many of these gaps among C-SCRM practices and general supply chain visibility among critical infrastructure asset owners and operators.

***

Again, the OT Cyber Coalition thanks NIST for the opportunity to provide feedback that should inform the important work your organization is undertaking to protect all of our nation's ICS and OT environments, not just those involved with critical infrastructure sectors. We welcome questions on our feedback and look forward to continuing to be a part of this discussion as it develops.

Sincerely,

Andrew Howell
Operational Technology Cybersecurity Coalition
[redacted]
https://www.otcybercoalition.org