As of: 4/11/22 8:45 AM
Received: April 11, 2022
Status: Pending_Post
Tracking No. l1u-of7d-gqiq
Comments Due: April 25, 2022
Submission Type: Web

PUBLIC SUBMISSION

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-0018
Comment on FR Doc # N/A

Submitter Information

Organization: Praetorian Security Inc.

General Comment

See attached document, comments in blue text, original requests in black text.

Attachments

NIST CSF RFI.docx

Background: Praetorian performs NIST CSF assessments for our clients and has tried to stay as close to the intent of the CSF as possible. We have certainly made additions to the CSF to make it work for our clients and many of those additions are detailed below. Since 2018 we have conducted NIST CSF assessments for approximately 20 clients ranging from 300 person organizations to Fortune 100 enterprises.

Responses have been copied between prompts where appropriate.

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 five functions are a logical and useful way to break up risk management for organizations. That being said, we have noticed a few shortcomings:

- The Respond and Recover functions are almost always repetitive in most organizations. Although at a low level there is a clear difference between the two, we find that in all but the most mature organizations, they are effectively the same functions.
- The Identify function has several subcategories that overlap greatly with subcategories in Protect and Defend. Although at a low level there is a clear difference in the intent (defining things vs. actually doing them), there seems to be a lot of repetition. One example is around threat and vulnerability identification. This shows up in Identify but then again in Protect with only a slight variation. More examples can be provided if necessary.
- While the 5 Functions are a logical way to organize the framework, mapping the functions from the CSF to organization functions (or business units) is near impossible. As a result, single individuals, org functions, or business units often have responsibility for subcategories across all 5 functions. This makes the assessment and management of the framework quite difficult. Although all organizations are different, we believe that there is a “best guess” list of common organizational functions that **most** organizations have whether as a dedicated role, business unit, or additional duty.
- We have found that simply assessing at the subcategory level is not adequate for most organizations. We have adopted a People, Process, and Technology assessment approach on a per subcategory basis to help organizations better understand the shortfall. Simply assessing a subcategory as not implemented is not useful to an organization as more information is needed to determine the root cause for the lack of implementation. Taking this one step further, organizations may have vastly different implementation levels across different environments (cloud, on-prem, client devices, network devices, etc.).

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?

- Much of the framework is implemented by most organizations at some level. The major limitation for most organizations is the **degree** to which they have implemented the various subcategories. A relevant metric that would aid in noticeable improvement would be something to determine the maturity of implementation. We use the Capability Maturity Model, but others may also suffice. No subcategory is implemented in a yes/no or true/false model. They are all implemented along a spectrum.
- We find that in most cases, the strategic recommendations from our NIST CSF assessments are similar or the same. Most organizations fail in a few common areas and tend to have others well implemented without needing further assessment or assistance.
    - Technology-based subcategories (primarily in Protect and Defend) tend to be well implemented in most organizations and do not benefit much from the application of the CSF. Again, they could improve maturity, but these subcategories are usually implemented at an adequate level.
    - Asset management is a common issue for most organizations as such, ID.AM often provided benefits.
    - Accounting of risk through a risk register or similar tool is a common issue for most organizations as such, ID.RA and ID.RM often provided benefit
    - Respond and Recover tend to be well implemented but the inclusion of the Public Relations aspect does often provide benefit to an organization that may not have included that part of planning in their Incident Response plans.
- For cybersecurity organizations that are understaffed, underfunded, full of technical debt, and being asked to do more daily, the NIST CSF provides a way to prioritize work. The degree of maturity for the various subcategories can also help organizations understand where to shift resources for the greatest improvement.

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).

- Much of the framework is implemented by most organizations at some level. The major limitation for most organizations is the **degree** to which they have implemented the various subcategories. A relevant metric that would aid in noticeable improvement would be something to determine the maturity of implementation. We use the Capability Maturity Model, but others may also suffice. No subcategory is implemented in a yes/no or true/false model. They are all implemented along a spectrum. Having a defined rating/scoring/maturity model would also help with information sharing across organizations (i.e., how do we compare in our industry, with our peers, etc.)
- Organizations (right or wrong) want a grade or a score. Since the NIST CSF does not dictate a scoring mechanism, this is difficult to provide without developing something internally.
- The CSF currently lacks adequate coverage for software development. Although you can pigeonhole many subcategories to make this work, it is not ideal.
- While the 5 Functions are a logical way to organize the framework, mapping the functions from the CSF to organizational functions (or business units) is near impossible. As a result, single individuals, org functions, or business units often have responsibility for subcategories across all 5 functions. This makes the assessment and management of

the framework quite difficult. Although all organizations are different, we believe that there is a "best guess" list of common organizational functions that **most** organizations have whether as a dedicated role, business unit, or additional duty.

- Either self-assessing or getting an external assessment against the CSF requires significant resources. This itself is not a challenge but there could be more or better resources showing how organizations can implement the CSF in practice and in a way that maximizes resource value. For example, self-assessment schedules, assessment metrics/criteria, or best practices might be useful for organizations.

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 CSF needs more coverage for software/application development, from somewhere like the NIST Secure Software Development Framework or Google's SLSA Framework.
- The PR.MA category does not apply to many/most organizations. Most orgs are not performing maintenance and instead are relying either on cloud assets, vendor-provided maintenance, or datacenter CoLo agreements for maintenance. There should still be a subcategory for this but probably not a full category.
- The use of Tiers needs more clarification. The principle seems sound but in implementation, the Tiers are confusing and hard to work with. Are Tiers meant to be assessment criteria or just a way to frame conversations about the CSF?
- The concept of Profiles makes sense. The Current and Target state profile concepts are easy to digest. However, since "This Framework does not prescribe Profile templates, allowing for flexibility in implementation," many organizations are left to figure it out on their own without much guidance.
- The references to Critical Infrastructure nullify many subcategories for organizations that do not provide critical infrastructure services. The requirements for cybersecurity are the same for all organizations regardless of relation to critical infrastructure. Relation to critical infrastructure should drive higher maturity targets (target state) rather than a different set of baseline requirements.
- The Respond and Recover functions should include common business requirements such as Business Continuity Plans and the inclusion of RTO/RPO metrics in the BCP and other recovery plans/processes.

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.

- Many organizations utilize the CSF on an ongoing or annual basis. Backward compatibility is crucial for organizations to measure progress. If backward compatibility is not possible, at the very least, an accounting of changes and a mapping between versions will be necessary. The CIS just did this with their major update to their Controls and moving from 20 to 18.

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

- We would be remiss if we did not try to include cloud-native technologies and micro-services in future updates to the framework. While many subcategories apply independent of the platform in question, there are special security considerations for these “new” additions to the IT landscape.

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.

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?

While the mapping between different frameworks or approaches is useful, organizations that are trying to do a crosswalk between them are likely better served to use tooling/software to support a secure-once/comply-many approach. Also, NIST needs to commit to keeping the mappings up to date as the other frameworks/approaches make their own updates.

For the most part, we see few if any conflicts and largely see commonalities or differences in coverage between differing approaches.

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 have applied the CSF internationally without any modification specifically designed to address the international community. If anything, the CSF utilizes a US-centric definition of critical infrastructure that could be expanded but realistically, it can still be applied as-is.

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. Start Printed Page 9581

No Comment

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?

- Better definitions of what or which supply chains are being referenced in a given control/category are necessary. Also, definitions about whether references are to supply chain consumers or providers. Does supply chain reference just physical material or also software? What about software development processes that are considered a supply chain? “Supply Chain” is an extremely broad term that needs better scoping/definition. Google’s SLSA framework is a great accounting of the entire software supply chain.

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.

- Google’s SLSA framework, slsa.dev

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?

- No comment

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.

- Almost every sub-category in the CSF could benefit from additional guidance. Supply-chain considerations is one area of many. This is simply to say that integrating the framework with additional guidance is useful here and elsewhere.