Cybersecurity Coalition

May 29, 2023

VIA EMAIL: cyberframework@nist.gov

Cybersecurity Framework
National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

Comments on the "*NIST Cybersecurity Framework 2.0 Core Discussion Draft*"

The Cybersecurity Coalition ("Coalition") is pleased to submit our comments in response to the discussion draft of the NIST Cybersecurity Framework 2.0 Core.[1] The Coalition is composed of leading companies with a specialty in cybersecurity products and services, who are dedicated to finding and advancing consensus policy solutions that promote the development and adoption of cybersecurity technologies. We seek to ensure a robust marketplace and effective policy environment that will encourage companies of all sizes to take steps to improve cybersecurity risk management.

The Coalition is broadly supportive of the proposed changes to the CSF 2.0 Core. We appreciate the agency's willingness to work alongside industry to adapt the CSF to be increasingly useful and applicable for entities of all sizes. The Coalition would like to express its support and offer further recommendations on the following topic areas:

1. Governance Function
2. Reorganization of Categories and Subcategories
3. Inclusion of Implementation Examples
4. Broadening Beyond Critical Infrastructure
5. Traceability Matrix
6. Engagement with International Partners
7. Online tools for Informative References

[1] https://www.cybersecuritycoalition.org/

1. Governance Function

The Coalition supports the addition of the Governance function to the Framework Core. Robust security risk management practices must incorporate governance processes to manage and monitor an organization's regulatory, legal, risk, environmental, and operational requirements. The addition of a Governance function in the Framework Core will highlight the importance of defining roles and responsibilities, prioritizing and assessing relevant risks, and integrating policies and procedures to enable a successful risk management program.

2. Reorganization of Categories and Subcategories

The updated Framework Core appears to reorganize the categories and subcategories to follow a pre-incident and post-incident chronology. The Coalition supports this intuitive reorganization and believes it may help small and medium size businesses to more effectively implement the CSF guidance. This change positively reflects the desire of NIST to address the needs of all organizations using the CSF regardless of their sector type, size, or maturity levels.

3. Inclusion of Implementation Examples

The Coalition is also supportive of including implementation examples to provide concise, action-oriented steps to help achieve the outcomes of the CSF subcategories. The Coalition believes implementation examples would be helpful either in the Core itself, or as an appendix. The examples should provide clear guidance on achieving the outcomes of the subcategories for a variety of organizations and sectors to diversify the applicability of the CSF. The Coalition urges NIST to collaborate with industry to identify and articulate practical examples that would be most useful for NIST Framework users.

4. Broadening Beyond Critical Infrastructure

The Coalition supports the removal of references to critical infrastructure to clarify that the CSF can be used by both critical and non-critical infrastructure organizations. As a practical matter, the CSF has been positioned and recommended as a risk management tool for non-critical infrastructure for several years. Making it clear that the CSF applies beyond critical infrastructure will help avoid confusion about its applicability and facilitate broader adoption.

5. Traceability Matrix

The Coalition appreciates that NIST provided traceability information with the proposed Core update, enabling users to quickly visually discern which categories, subcategories, and wording has changed. Highlighting these changes will help users determine where they should focus their attention, while also providing a sense of transparency to the revision process.

6. Engagement with International Partners

The Coalition encourages NIST to continue engaging with non-US governments to promote adoption of the Framework. International alignment on the CSF Core will help US and non-US partners aim at similar goals and consistently communicate on risk management practices. Direct engagement with foreign governments and industry can help inform potential changes to new iterations of the CSF and educate on international adoption. The CSF is already highly regarded and frequently referenced in other global cyber strategies. Continued consultations with international partners will further this momentum in aligning cybersecurity practices worldwide.

7. Online Tools for Informative References

Finally, the Coalition would like to echo our previous comments and encourage NIST to explore ways to provide online tools for informative references that meet the needs and capabilities of the entire community using the Framework.[2] The NIST Cybersecurity and Privacy Tool (CPRT)[3] and the Online Informative References Program (OLIR) Catalog[4] are complex programs that pose a barrier to CSF users who are unfamiliar with these tools. As NIST transitions to these dynamic tools, it is critical to ensure that they are as usable as having a set of informative references directly in the Framework document.

Historically, organizations have based their cyber risk management on a specific set of international standards or industry best practices. NIST should consider allowing current and prospective CSF users to generate self-contained and customized documents that map to standards and best practice documents they identify as being relevant to their organizations. Ideally users would be able to select a set of standards and/or industry best practices mappings and then generate a copy of the CSF 2.0 (or other NIST framework document, such as the Privacy Framework) with the Informative References section of the Framework Core filled in with the user-selected set of mapped references.

We suggest that this capability should also enable printing a complete self-contained version using open standard formats, such as XLSX, JSON or PDF. This would allow organizations to distribute a complete copy internally to their cyber risk management stakeholders, as was initially available in the 1.0 and 1.1 version of the CSF. A new version could always be regenerated whenever a new or updated applicable standard or best practice document was added to the online references tool. We believe this would best satisfy the global community of

---

[2] https://www.cybersecuritycoalition.org/filings/comments-on-the-nist-cybersecurity-framework-2-0-concept-paper-potential-significant-updates-to-the-cybersecurity-framework

[3] https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_1_1_0/home

[4] https://csrc.nist.gov/projects/olir/informative-reference-catalog

stakeholders by making the CSF (or other related NIST framework documents) more readily consumable in a manner customized to be more relevant to the needs of the individual organization.

Thank you!

The Coalition appreciates that NIST continually listens to the private sector and thanks NIST for allowing us to contribute our thoughts and recommendations to the dialog. As the conversation around this topic continues to evolve, we would welcome the opportunity to further serve as a resource on both technical and policy questions to ensure that Cybersecurity Framework continues to be successful in driving consistent, effective cyber risk management practices globally.

Respectfully submitted,

The Cybersecurity Coalition