March 17, 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 Concept Paper: Potential Significant Updates to the Cybersecurity Framework*'

The Cybersecurity Coalition ("Coalition") is pleased to submit our comments in response to the NIST Cybersecurity Framework 2.0 Concept Paper. 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.

There are four areas the Coalition would like to provide comments on:

1. Develop Community-Centric Online Tools to Map CSF Core Subcategories to Informative References;
2. Enable Targeted Updates to Subcategory Informative References;
3. Continue Existing Efforts to Incorporate Supply Chain Risk Management into the CSF Core;
4. Architectural Review - Incorporating Additional Frameworks with the CSF Core.

1. Develop Community-Centric Online Tools to Map CSF Core Subcategories to Informative References

The NIST Cybersecurity and Privacy Tool (CPRT) and the Online Informative References Program (OLIR) Catalog are complex programs that may be a barrier to understanding for some CSF users. We recommend NIST explore ways to provide online tools for informative references that meet the needs and capabilities of the community.

In section 2.3 and 2.4, the concept paper describes the problem of having static informative references. This occurs when the referenced standards or best practice documents are updated. It also states the Informative References listed in previous versions of the CSF are only a small subset of the standards that could be leveraged by organizations. We agree this does need to be addressed. The standards and documented best practices are updated frequently and not on the same timeline as the CSF. There are many standards and documents that could be referenced and

listed but NIST picked an initial set representative of national and international standards and industry best practices at the time of publication.

As described, NIST's proposed solution is to use CPRT and OLIR. Putting Informative Reference data online, where it could be much more dynamically updatable, is a potentially valuable capability for the global community of users who manage risk consistent with the CSF. However, while we understand the purposes of CPRT and OLIR online tools, we question the capabilities they provide for the user community. Today, it appears the two tools are there for how NIST manages documents and accepting the submission of mapped informative references. They do not appear to provide support for the community who would use them. For the intended purposes of providing Informative References mapped to the actual subcategories, the current online capabilities are lacking in their usefulness.

We have found having a set of informative references directly in the Framework document is valuable to those actively reading and using it. During the Privacy Framework development, it was decided to NOT have a set of base level informative references included in the Privacy Framework 1.0. We have heard multiple times this makes it harder to use and highly dependent on the OLIR. ***This is because people have to learn how to use the CPRT and the OLIR in order to get what was intended for these tools to deliver.*** Finding a base set or any specific set of standards and best practice mappings is now an adventure in clicking. While the foundation for accomplishing what NIST's solution proposes exists, there just seems to be something fundamental missing.

Recommendation:

Historically, organizations have based their cyber risk management on a specific set of international standards or industry best practices. We believe that the result being sought by NIST would be best achieved by 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. We therefore request NIST consider enabling CSF users to be able to select a set of standards and/or industry best practices mappings and then provide a means for the user to generate a copy of the CSF 2.0 (or maybe another NIST framework document, such as the CSF 1.1 or the Privacy Framework). The generated document would contain the ***full text***, and the ***Informative References section of the Framework Core*** filled in with the ***selected set of mapped references***.

This capability should provide for printing a complete self-contained version using open standards, 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. The generated copy could be marked as generated by the CPRT with machine readable version information. This would supply all the text and the Framework Core together, with the selected Informative References current as the date of generation, in a highly convenient version for local needs and use. 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 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.

Taking the Informative References out of the CSF document and moving them to an online tool makes it harder for organizations to map their existing practices to the CSF. This means more work for an organization just trying to understand the subcategories. By allowing selection of the appropriate mapped standards or best practice documents, organizations would be able to generate a copy matching the standards and best practices they are already using. Our recommended approach would make adoption easier, individual organizational needed information more accurate, and have it all in one place.

We recognize and agree with NIST's concern that Informative References included in the Framework may become stale and dated. However, by enabling organizations to generate their own Framework Core customizable to reflect the risks, standards, and controls relevant to their operations, both NIST and the CSF user community gets what is needed, timeliness, accuracy and useability.

2. **Enable Targeted Updates to Subcategory Informative References**

The current process used by NIST to accept suggested mappings and corrections to Informative References seems to be essentially an "all or nothing" proposition. While for the most part this makes sense, having the capability to map specific references to specific subcategories is also needed. For example, the RS.AN-5 Informative References have little to do with the globally recognized coordinated vulnerability disclosure process this subcategory is addressing. The Informative References for RS.AN-5 need to be corrected to reflect the internationally recognized ISO/IEC 29147 and ISO/IEC 30111 standards. Our members believe there needs to be a mechanism allowing for a targeted update to a specific or individual sets of Informative References, short of mapping to an entire document. While this is a single example, it is representative of an update capability needed for NIST documents with online references. Spot correction capabilities are needed. The Coalition and others have requested the updates to RS.AN-5 in the past. We recommend that NIST develop a spot correction capability in the next version of the CSF—or if it currently exists more clearly explain how the process works.

3. **Continue Existing Efforts to Incorporate Supply Chain Risk Management into the CSF Core**

While supply chain attacks have been successful, we do not believe there is a need to create an entirely new supply chain top-level Function. C-SCRM would be better integrated within the existing CSF subcategories, with the potential for new subcategories as required. With the development and agreement of a new GOVERN Function, C-SCRM has another appropriate place to be addressed.

At the In-Person February CSF Working Sessions, the topic of SBOM inclusion came up. SBOMs in the CSF should be included as software build artifacts, if needed to be specified at all. They should not be included directly in the Framework. The Coalition believes it is important to continue to assure the CSF 2.0 remain technology and vendor neutral. In our view, it would be more effective to continue leveraging the current approach of adding C-SCRM elements to existing functions—including, if appropriate, secure software development artifacts instead of building out a new core function for this purpose.

4. **Architectural Review - Incorporating Additional Frameworks with the CSF Core**
The Cybersecurity Framework has touched a lot of areas in its going-on ten-year history. As noted above, the community of stakeholders is truly global. The Framework effectively serves as the source for baseline voluntary guidelines and tools aimed at small and medium sized business, including DHS CISA's Cyber Performance Goals. It is even used as the methodology for ensuring compliance with mandatory regulatory regimes, including the U.S. federal government's requirement to leverage the CSF in the course of complying with the law that ensures the security of federal information systems.[1] As NIST is also well-aware the Framework has been translated and used by governments in many countries.[2]

   At the same time, NIST has attempted to build on the success of the CSF by developing additional frameworks, which vary in their structure from the original.[3] Section 2.2 in the 2.0 Concept paper recognizes this issue and discusses the need to relate the CSF clearly to other frameworks. We suggest that NIST undertake an effort to review the architecture of the CSF and related initiatives to ensure an approach that is as reasonably consistent as possible across them to better enable effective adoption, implementation, and use.

   Beside these NIST documents, there are other evolving and emerging areas that need to be properly addressed. For example, these currently include IoT, OT, Product Lifecycle, Cloud, Zero Trust, AI, and more that will be generated over the near future that are just as important to be clearly related in some fashion to the CSF.

   We believe with the mix of topics and NIST related frameworks trying to be addressed in CSF 2.0, it is time to step back and consider an overall architectural approach to adding/linking other frameworks to CSF. It may be the CSF could be the "Core" with a family of directly related frameworks. For example, there could be a more in-depth Product Lifecycle Framework incorporating the SSDF. Not all companies sell software. But for those that do, a Product Lifecycle Framework could be useful. It may be worth considering whether and how such an approach might fit into the CSF family of risk management frameworks. In our view, the CSF could potentially serve as the keystone allowing a bridge between the various risk management frameworks that NIST manages As such, there needs to be discussions on how best to address areas closely related.

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.

---

[1] Executive Order 13800, https://irp.fas.org/offdocs/eo/eo-13800.htm
[2] NIST's website lists 9 translations of the CSF from Arabic to Ukrainian.
https://www.nist.gov/cyberframework/framework
[3] NIST's website lists: 1. Privacy Framework; 2. NICE Framework for Cybersecurity; 3. Risk Management Framework; 4: Cybersecurity Framework; and Secure Software Development Framework.

Respectfully Submitted,

The Cybersecurity Coalition