April 25, 2022

Submitted via email to CSF-SCRM-RFI@nist.gov

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

Subject: RFI: Evaluating and Improving Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management

The Information Technology Sector Coordinating Council (IT SCC) appreciates the opportunity to provide comments on the National Institute of Standards and Technology (NIST) Request for Information (RFI) on evaluating and improving cybersecurity resources, including with regard to the *Framework on Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework) and for the recently announced cybersecurity supply chain risk management initiative.

The IT SCC was established in 2006 to bring together companies, associations, and other key IT sector participants to coordinate strategic activities and communicate shared views. As corporate entities managing risks for ourselves and our customers, and as a sector collaborating with the government to assess and manage risks, the IT SCC has considerable experience with cybersecurity resources.

We appreciate the collaborative process that NIST leverages to develop and evolve cybersecurity resources, and we support further efforts by NIST to ensure that next steps for both evolving the Cybersecurity Framework and developing the cybersecurity supply chain risk management initiative reflect an inclusive and iterative approach (see Sections I and VI). In addition, we offer recommendations related to the content of the Cybersecurity Framework (see Sections II and III) and ways to strengthen interoperability with other resources and adoption of its practices, both domestically and internationally (see Sections IV and V). Finally, we offer recommendations regarding the scoping and approach of NIST's cybersecurity supply chain risk management initiative (see Section VI).

In summary, we recommend that NIST:

- Leverage an inclusive and iterative process for evolving the Cybersecurity Framework, allowing time for meaningful engagement and exchange with diverse communities domestically and internationally, including through hybrid workshops;
- Update the Cybersecurity Framework Core to reflect developments in supply chain security, threats across different technology environments, and vulnerability management;

- Update the Cybersecurity Framework's approach to Implementation Tiers and Profiles as well as metrics and ways to benchmark against peers and measure continuous improvement;
- Improve interoperability and alignment with other resources and references, creating greater clarity and simplicity for risk management and compliance efforts;
- Promote greater adoption and use of the Cybersecurity Framework both domestically and internationally, including through an inclusive and iterative process for evolving the Cybersecurity Framework, additional guidance to support various communities and use cases, and incentives; and
- Build upon industry efforts to define frameworks or standards for describing supply chain security and exchanging verifiable supply chain artifacts.

While we are supportive of NIST's effort to ensure that the Cybersecurity Framework remains an up-to-date resource, we also believe that foundational principles have been critical to its success and will continue to be relevant going forward. Simplicity and flexibility are key among those principles. By simplicity, we refer to the organization of the Cybersecurity Framework Core, the high-level Functions of which provide a straightforward way to think about and organize cybersecurity risk management. By flexibility, we refer not only to the way users can determine what functional areas and practices apply to them but also to how the Cybersecurity Framework can be leveraged for enterprise risk management, customer engagement, and other purposes. We also refer to how the Cybersecurity Framework can be overlaid with existing risk management processes that can complement and/or improve Framework-based processes. The Cybersecurity Framework's flexibility, along with its voluntary nature, has allowed it to be leveraged effectively in a regulatory context in certain sectors and regions.

I. Developing the Cybersecurity Framework Version 2.0 through a high-engagement model and an inclusive and iterative process

The IT SCC has long supported NIST's perspective that the Cybersecurity Framework should be a "living document...to address constantly evolving risks to critical infrastructure cybersecurity."[1] The IT SCC also previously supported the improvements and additions made to draft Version 1.1, recognizing them as "necessary and timely" while also advocating for ongoing flexibility in how organizations use the Cybersecurity Framework, recognizing vast diversity in readiness and resources across the ecosystem.[2]

As a continuation of NIST's effort to make sure the Cybersecurity Framework is a "living document," the IT SCC again supports NIST's current initiative to evaluate whether and how to add to or otherwise improve it as a resource. Furthermore, given developments in the technology and threat landscape since the Cybersecurity Framework was last updated, we agree that a significant update, to "Version 2.0," is warranted. However, the process that NIST undertakes to update the Cybersecurity Framework will be critical to ensuring its relevance across the ecosystem and to maximizing potential positive impacts.

---

[1] Federal Register, *Developing a Framework To Improve Critical Infrastructure Cybersecurity* (Feb. 26, 2013), https://www.federalregister.gov/articles/2013/02/26/2013-04413/developing-a-framework-to-improve-critical-infrastructure-cybersecurity; IT SCC Comments to NIST (2013), https://www.nist.gov/system/files/documents/2017/06/12/20131220_angela_mckay_itscc.pdf.

[2] IT SCC Comments to NIST (2017), https://www.nist.gov/system/files/documents/2017/04/20/2017-04-10_-_itscc.pdf.

NIST should embark on an inclusive and iterative process, allowing time for meaningful engagement and exchange with diverse communities domestically and internationally, including through hybrid workshops that allow for in-person and remote participation. The participation model that NIST leveraged in developing the Cybersecurity Framework Version 1.0, including in-person workshops in geographically distributed locations and multiple RFIs, enriched both the content of the Cybersecurity Framework and awareness and adoption of its practices. Leveraging a similar model for a more significant update to Version 2.0 – instead of the more streamlined process that NIST used for Version 1.1 – will similarly allow NIST and stakeholders to deliberate together on thoughtful input to challenging but important questions, such as how to integrate supply chain risk management more holistically, support use of the Cybersecurity Framework for measuring continuous improvement, and promote and simplify adoption.

II. Updating the Core of the Cybersecurity Framework Version 2.0

The IT SCC welcomes NIST's interest in further integrating supply chain risk management into the Cybersecurity Framework 2.0 and otherwise updating Core content to reflect the ongoing evolution of the technology and threat landscape. We consider the following areas to be relevant for substantive updates and offer the following initial recommendations as input for the next phase of deliberation in what we hope will be an iterative process.

Supply chain risk management

Over the last two years, supply chain attacks have grown in prominence, resulting in increased recognition of the importance of efforts to enhance supply chain risk management. In addition, Executive Order 14028 was issued, and NIST and others have developed or evolved numerous supply chain security resources, such as the NIST Secure Software Development Framework (SSDF).

The IT SCC supports going beyond NIST's approach to integrating supply chain security in the Cybersecurity Framework Version 1.1. NIST's goal should be to address increasing risk while maintaining simplicity and flexibility. Across the Protect, Detect, Respond, and Recover Functions, supply chain risk management practices are relevant. More specificity is also needed regarding supply chain risk management efforts in different contexts, such as for hardware versus software, development versus acquisition, and IT versus operational technology (OT) products (given radically different lifespans).

The IT SCC especially encourages NIST to consider how to incorporate secure software development practices into the Cybersecurity Framework. Even organizations that are not software vendors have internally developed software used for mission-specific or integration purposes, and all software should be following secure development practices and leveraging a process to document those practices. We anticipate that adding new Categories and/or Subcategories as well as the SSDF as an Informative Reference could be an appropriate way to strengthen alignment and clarify the relationship of the Framework Version 2.0 with Executive Order 14028 Section 4 requirements, though we also note that it will be important to limit confusion of organizations currently using the Framework regarding security practices applicable to software development versus acquisition.

Executive Order 14028 Section 4 is also prompting new efforts related to software supply chain transparency, including requirements for federal software vendors to provide Software Bills of Material (SBOM) information. While there are many ongoing questions, especially related to the delivery, storage,

and use of SBOMs, that may make more challenging efforts to integrate SBOM practices from SSDF and other resources, we anticipate that doing so could be helpful in aligning resources and driving clarity.

However, as we also recognized in 2017, supply chain risk management efforts may unfortunately vary widely across differently situated organizations, including small and large businesses with disparate market levers and budgets.[3] Integrating supply chain risk management across the Cybersecurity Framework's Functions and with consideration of different contexts is necessary to align with security best practices and existing resources, but NIST should seek further feedback regarding how it can do so while maintaining its relevance across communities. For instance, for some organizations, integrating additional supply chain Informative References, such as NIST SP 800-161, could be helpful in supporting interoperability and alignment of resources. However, for small businesses, we also recognize that NIST SP 800-161 is overly complex. While we believe it is important to avoid multiple additional frameworks, such as a cybersecurity supply chain risk management framework, additional use cases, profiles, or guidance may enable NIST to drive greater clarity and alignment while maintaining broad user relevance.

Technology environment threat management

Since NIST last updated the Cybersecurity Framework, emerging technology has continued to proliferate and impact new organizational functions and missions. As a result, the attack surface has also expanded for many critical infrastructure and other organizations. In this version 2.0 update, across Functions, NIST should contemplate how to highlight and address risks and risk management processes associated with connected assets across IT, OT, Internet of Things (IoT), mobile, and cloud environments. NIST could also consider how to integrate advanced Artificial Intelligence (AI)/Machine Leaning (ML)-based threat prevention, detection, and response as enhancements to the Protect, Detect, and Respond Functions.

Vulnerability management

Developing and implementing a vulnerability management plan has long been recognized by NIST and others as critical to cybersecurity risk management (including in the Cybersecurity Framework Version 1.1 Subcategory PR.IP-12). However, recent attack trends and recognized gaps in risk management activity have demonstrated the ongoing importance of not only implementing a general plan but also prioritizing management of vulnerabilities that pose an elevated threat. For example, given ongoing threats and awareness of risk management practices, the Cybersecurity and Infrastructure Security Agency (CISA) has recently established priorities for vulnerability management on behalf of federal civilian agencies.[4] The IT SCC likewise recommends that NIST strengthen its guidance on vulnerability management to ensure that organizations focus on mitigating vulnerabilities that pose the greatest threat based on factors such as severity, exploitability (including vulnerabilities for which there are already exploits available), and asset criticality.

III. Updating how the Cybersecurity Framework Version 2.0 fosters the use of metrics and measurement and drives continuous improvement

---

[3] *Id.*

[4] *CISA Releases Directive on Reducing the Significant Risk of Known Exploited Vulnerabilities,* https://www.cisa.gov/news/2021/11/03/cisa-releases-directive-reducing-significant-risk-known-exploited-vulnerabilities?msclkid=fa8ef4e4aed611ecb8905a2cdf9dbdcd (last revised Jan. 24, 2022).

As discussed above, one of the Cybersecurity Framework's greatest strengths is its foundational flexibility, making it a great starting point and continuous improvement tool for a variety of organizations looking to assess and strengthen their cybersecurity risk management posture. The IT SCC has previously noted and continues to acknowledge that "maintaining flexibility in the application for organizations will be critical to continued use and adoption of the Framework."[5] However, the flexibility of the Cybersecurity Framework can also sometimes result in organizations struggling to achieve the full potential value of assessments.

The IT SCC believes an appropriate balance can be struck that maintains an accessible, flexible process with further metrics and anonymized benchmarking that can help organizations get a better understanding of their own cybersecurity posture based on their risk assessment. We appreciate that the Cybersecurity Framework Version 1.1 tried to address this issue with a robust restatement of the purpose of the Cybersecurity Framework and a section on self-assessment and metrics. However, further focus on these topics can result in additional improvements in Version 2.0.

Improving Tiers and Target Profiles

The IT SCC recommends that NIST consider ways to make Section 2.2, *Framework Implementing Tiers,* and Section 2.3, *Framework Profiles,* more robust and useful to organizations. As written, it is not clear how the Tiers and Profiles are intended to be used nor when and how an organization should determine its current Tier/s across Core practices or develop its Target Profile.

NIST should provide more information about why the Tiers are important as well as include more substance about each Tier to help organizations determine their status (including people, processes, technology, and other considerations). NIST should also provide more information about how each Tier can be achieved as guidance for those organizations looking to improve.

Similarly, NIST should provide more information about the purpose of the Target Profiles and how an organization can assess what its target state ought to be given the level of risk the organization is able to accept. We also suggest that NIST underlines the various ways in which organizations might develop, apply, or otherwise use Target profiles, recognizing the importance of flexibility as well as the challenges that some organizations have faced in developing Target profiles at the outset of using the Framework. While crafting targets at the outset of Framework implementation could help organizations better determine what gaps need to be addressed, earlier on in the process, they may also have less context to understand how Tier assessment should be made as well as where and to what extent to prioritize risk management improvements. Gaining that context after initial assessments are completed may allow for a more grounded and less overwhelming process of Target Profile development.

Improving Self-Assessments and Metrics

IT SCC recommends that the Cybersecurity Framework remain a flexible assessment tool. However, we also recommend that NIST consider ways to improve implementers' ability to assess whether they have met the specific cybersecurity outcomes in the Core Subcategories by: (1) considering ways to provide anonymized benchmarking or other case studies so organizations can have a more objective way to

[5] IT SCC Comments to NIST (2017), https://www.nist.gov/system/files/documents/2017/04/20/2017-04-10_-_itscc.pdf.

assess where they stand compared to other similarly-situated organizations; and (2) improving the usefulness of the Informative References supplied.

In 2017, the IT SCC suggested that NIST develop a series of case studies as a supplement to the Cybersecurity Framework. We noted that "[e]ach case study should be based on real world examples and reflect the efforts to implement the Framework for small, medium and large companies."[6] We continue to believe that having case studies or some form of anonymized outputs from organizations who have gone through the Cybersecurity Framework process, classified by industry and size, will help organizations more accurately and appropriately assess their risk posture.

NIST should also consider ways to improve guidance for organizations about how to meet expectations for some of the larger, more weighty Subcategories – such as activities that, at a minimum, an organization could perform to achieve its outcomes. Such an approach would allow the Cybersecurity Framework to continue to leverage an outcomes-focused approach while providing clearer implementation examples for those organizations that would benefit from additional guidance. In the alternative, if Subcategories do not include specific examples of activities or implementation approaches, we suggest NIST consider how to improve the usefulness of its Informative References by providing tiered categories to guide implementers, such as authoritative and informative references. Today, some implementers use the Informative References as authoritative – complete references that outline the controls that need to be implemented to meet the Subcategory – which NIST may not have intended. Providing tiered references could help companies prioritize controls relevant to the Subcategories.

IV. Strengthening interoperability and alignment of the Cybersecurity Framework Version 2.0 with complementary resources

The IT SCC recommends that NIST closely evaluate how the Cybersecurity Framework Version 2.0 aligns with and integrates other authoritative resources, both from NIST and other U.S. agencies. Since first publishing the Cybersecurity Framework, NIST has done a great deal of work developing risk management guidance, assessments, and other resources, as have other federal agencies. Depending on which sector an organization operates in, to whom the organization sells its services, and what technology environment is at issue, the organization could have dozens of federal resources potentially at play, and many more if it is a multinational organization. The sheer number of these sources can be overwhelming, particularly for small and medium-sized organizations. It can also be difficult to understand how each resource complements others and when and how they should be used together.

In addition to the SSDF and Executive Order 14028 discussed above, NIST should also make clear how the Cybersecurity Framework aligns with NIST's risk management and privacy frameworks and resources focused on integrating cybersecurity and enterprise risk management, among others. Current and in-development programs like FedRAMP and the Cybersecurity Maturity Model Certification (CMMC) further complicate this issue for some organizations, raising questions about how these frameworks and certifications can align. To maximize the usefulness of investing in using the Cybersecurity Framework, NIST can help ensure that all these resources work together in a coherent way as building blocks to meet organizations' needs. The Cybersecurity Framework could even be a tool to help organizations prepare for CMMC, recognizing the value of the Framework for security versus CMMC for compliance. Overall, the Cybersecurity Framework could function as an organizing mechanism (i.e., a "hub") to bring security

[6] *Id.*

focus to compliance efforts (i.e., "spokes"). Where requirements exist, linking those with Cybersecurity Framework subcategories could help everyone use consistent language.

The IT SCC recommends that NIST consider specifically how CISA and NIST's cybersecurity performance goals, developed pursuant to the President's Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems, could be incorporated into or aligned with the Cybersecurity Framework.[7] Initial comments from industry to CISA on its first draft of baseline performance goals focused heavily on questions about what value the initiative offers. When recently asked how the performance goals complement other frameworks and standard initiatives, Executive Assistant Director for Cybersecurity Eric Goldstein described them as helping to answer the question of "how am I doing" as an organization and helping to provide a "set of benchmarks and baselines" and "outcome-based goals."[8] We understand that CISA and NIST will be continuing the refinement process to develop baseline standards and also plans to develop industry-specific performance goals. NIST should consider whether it would be useful to work with CISA to develop performance goals that could be added as authoritative references for Core Subcategories or whether they can be otherwise mapped to the Cybersecurity Framework in a way that provides maximum value and ensures they can be used coherently along with the Cybersecurity Framework by organizations.

V. Promoting adoption of the Cybersecurity Framework Version 2.0

The IT SCC appreciates NIST's ongoing focus on not only ensuring the Cybersecurity Framework is broadly useful and relevant for organizations but also helping them understand how to use it effectively. We have previously underlined that the Cybersecurity Framework's "domestic and international relevance" are foundational to improving cybersecurity "while maintaining and promoting innovative open markets for the benefit of all" and supported "increased promotion of the Framework" through active sharing "with international governments, standards organizations, and industry sectors."[9]

The IT SCC encourages NIST and U.S. government partners to invest significantly more resources in promoting the adoption and use of the Cybersecurity Framework internationally. As part of this effort, NIST should be resourced to ensure that international stakeholders – including governments, industry, and civil society – have an opportunity to participate meaningfully in the development of the Cybersecurity Framework Version 2.0. As part of a high-engagement model and inclusive and iterative process, workshops should either take place outside of the United States or be accessible to or even target international participation. In addition, NIST should work with international stakeholders to continue to promote the Cybersecurity Framework in the development and evolution of international standards.

Across all organizations and jurisdictions, further guidance from NIST on how to use the Cybersecurity Framework would also be helpful – along with efforts to promote existing, updated, and/or new

---

[7] The White House, *National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems* (July 28, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/.

[8] Operation Next:22 Conference (Mar. 23, 2022), https://accenture.touchcast.com/showtime/operationnext/join.

[9] IT SCC Comments to NIST (2013), https://www.nist.gov/system/files/documents/2017/06/12/20131220_angela_mckay_itscc.pdf; IT SCC Comments to NIST (2017), https://www.nist.gov/system/files/documents/2017/04/20/2017-04-10_-_itscc.pdf.

guidance. In particular, use cases and profiles could provide valuable implementation guidance. In addition, IT SCC organizations have either experienced or understood from others that there are significant challenges associated with getting started with the Cybersecurity Framework. In some cases, organizations have struggled to establish a "Target Profile" in advance and would benefit from guidance that prioritizes getting started and recognizes that such mechanisms to drive continuous improvement can be integrated as organizational processes mature. NIST could also help illuminate how the Cybersecurity Framework is different from or complementary to other control and compliance frameworks as well as provide context around how to use the Cybersecurity Framework versus its extensions, such as profiles for different sectors or types of threats.

NIST could also partner with other government stakeholders to incentivize use of the Cybersecurity Framework. Some states have pursued initiatives that may help drive use of the Cybersecurity Framework, including by leveraging tax credits or grant authorities. Public recognition for use of the Cybersecurity Framework, insurance benefits, or linkages between the Cybersecurity Framework subcategories and compliance requirements may also provide meaningful incentives. We encourage further exploration of what states or others have done as well as investments in strengthening interoperability and alignment to support broader adoption.

VI. Investing in improving cybersecurity supply chain risk management through NIST's new public-private partnership

The IT SCC is encouraged that NIST is establishing a new public-private partnership process to help organizations, including developers, providers, and acquirers of technology, to build, evaluate, and assess the cybersecurity of products and services. Tools, technologies, and guidance targeting these different communities have the potential to help accelerate organizations' ongoing supply chain risk management efforts, including for both software and hardware. As with the Cybersecurity Framework update, we encourage NIST to leverage an inclusive and iterative approach to building out this initiative, and we believe that industry partnerships, including through workshops or working groups, can help accelerate progress and drive impact.

To improve the trustworthiness of the supply chain, we would support efforts by NIST to define minimum guidance around the preparation, storage, distribution, consumption, and verification of attestations and evidence that are critical to maintaining the integrity of supply chains. Similar to the Cybersecurity Framework, such guidance should be sufficiently high level and flexible to accommodate multiple standards, best practices, and technologies. Existing industry-led efforts to define frameworks and standards for describing levels of software security and supply chain integrity or to enable the exchange of verifiable supply chain artifacts could also be built upon to the extent applicable.[10]

Thank you for the opportunity to provide comments and contribute feedback as NIST moves forward with its efforts to evaluate and improve cybersecurity resources, including with regard to the Cybersecurity Framework 2.0 and for the public-private partnership on Improving Cybersecurity in Supply Chains. The IT SCC is committed to supporting NIST and our other U.S. government partners as

[10] E.g., SSDF references as well as the projects like the Open Source Security Foundation (OpenSSF) Supply-chain Levels for Software Artifacts (SLSA), framework/slsa?msclkid=9ce3a324aedc11ecbb4be6429acca712, and the Internet Engineering Task Force (IETF) Supply Chain Integrity, Transparency, and Trust (SCITT), https://github.com/ietf-scitt?msclkid=020292bba6db11ec8569eadc629a068c.

these and other cybersecurity risk management initiatives move forward, and we look forward to our continued collaboration.

Sincerely,

Ari Schwartz
Chair, IT Sector Coordinating Council