SEEMLESS TRANSITION

4530 St John's Avenue
Suite 15 #340
Jacksonville FL, 32210

April 25, 2022

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

Re: Federal Register document 87 FR 9579 – "Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management"

Dear NIST team,

Seemless Transition LLC (STLLC) is proud to offer feedback to the Request for Information issued by the National Institute of Standards and Technology (NIST) on the topics of the Cybersecurity Framework (CSF) and cybersecurity supply chain risk management. STLLC is a consulting firm which focuses on standards-based approaches to cybersecurity risk management. Founded in 2020, we help our clients achieve efficient and effective cybersecurity programs through our experience in the standards space.

Based on STLLC's interaction with clients, we find the CSF to be a versatile tool for organizing and communicating about cybersecurity risk management. The value of the CSF continues to be the alignment of language across departments and organizations. The CSF continues to be the de facto standard for cybersecurity risk management.

Cybersecurity supply chain risk management continues to plague our nation. Recent attacks continue to follow common patterns which exploit the interconnectedness of our ecosystem. In order to mitigate risks to the overall cyber ecosystem, cybersecurity supply chain risk management must be addressed at every level of system and organizational structures.

In response to the RFI, we have left the statements as presented by NIST and supplied our experiences and thoughts beneath each statement.

1. **When your organization began using the NIST Cybersecurity Framework and how your organization uses it (e.g., to organize your efforts by the five functions as well as categories and subcategories, to actively manage your risks using the five functions, to create "to-be" vs "as-is" profiles and identify appropriate tiers).**

STLLC works with organizations to help create and maintain effective and efficient cybersecurity risk management programs. STLLC uses the CSF as a basis for that work. The

CSF Core provides a common set of outcomes which organizations can achieve through flexible implementation methods. The CSF allows STLLC to communicate across departments at our client's organizations using plain language to facilitate discussion of action items and monitor progress.

STLLC uses the CSF in conjunction with the CMMI Maturity Levels. By applying the CMMI levels at each subcategory, organizations can get fine-grained vision into the performance of their cybersecurity risk management programs.

Additionally, STLLC has produced a CSF profile which aligns the White House Fact Sheet on Cybersecurity (published 3/21/2022 at the below address [1]) to the CSF Core. This profile can be found at the below address [2]. This profile demonstrates the value of the CSF in organizing and communicating high level policy objectives. Furthermore, profiles such as this will continue to allow organizations to demonstrate their alignment to policy documents.

[1] https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/fact-sheet-act-now-to-protect-against-potential-cyberattacks/

[2] https://www.yourcyberwork.com/tools/profiles/whitehousefactsheet

2. **Primary benefits gained by your organization's use of the NIST Cybersecurity Framework (e.g., improved communications among various levels in your organization or with supply chain partners, customers, or insurers; better assessment of risks and potential ways to manage them, becoming more efficient and/or effective in managing risks). If relevant, please cite any metrics used to track implementation of the Framework and resultant improvements to cybersecurity.**

   The primary benefit of using the CSF is communication and organization of cybersecurity risk management programs. Using the CSF as a common language across and between organizations streamlines communication and eliminates confusion when discussing cybersecurity risk management. STLLC has experience using the CSF in conjunction with the CMMI Maturity Levels. By combining the two frameworks, STLLC can measure progress of clients. At varying snapshots in time, clients have been able to track their progress relative to their CMMI scores at each subcategory. Some clients roll these scores into CSF category scores. These scores have proven useful for communicating with board level stakeholders.

3. **Challenges that may have prevented your organization from using the NIST Cybersecurity Framework or using it more easily or extensively (e.g., resource considerations, organizational factors, workforce gaps, or complexity)**.

   1) *The CSF attempts to do too much* – The CSF is split into 3 separate components: the Core, the Tiers, and Profiles. Over the years, it has become evident that the Core is the most used portion of the CSF. Profiles have been created, and published, however, the dominant use of Profiles is for internal purposes. Concurrently, few resources which have been published use the Tiers. Coherent, repeatable, long term uses of the Tiers are few and far between. It is difficult to harmonize along both the Tiers and the Core. Therefore, it's difficult to use the CSF past the Core and Profiles.

2) *Parameterization of the CSF is difficult* – When attempting to track progress against any of the Core subcategories or the Tiers, finding reliable metrics remains a difficult endeavor. With respect to the Core, this difficulty is partly due to the design of "outcome statements" being organization- and technology- neutral. Therefore, they are flexible enough to apply to all organizations and contexts. The downside of flexibility is ease of implementation. While the Core subcategories are close enough to programmatic implementations, the Tiers remain out of reach for many.

   Concurrently, there is no standard way to measure each Core subcategory which is comparable ACROSS subcategories. Therefore, every measure is unique to the subcategory and the context in which the organization resides. This feature is difficult to "roll up" when discussing outcomes with executive level leadership. Not every subcategory is measured uniformly, therefore, not every Category can be compared. During engagements with clients the bottom line of "what's our score at a high level?" is a driving factor. With the current CSF, it is difficult to answer that question without many caveats.

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.**

While we still find the CSF a fantastic tool for helping organizations manage their cybersecurity risk management programs, there is room for improvement. In light of the difficulties we have had implementing and measuring with the CSF, STLLC provides following suggestions:

1) *Remove the Tiers* – While this may seem dramatic, it is a potential way to allow other NIST publications to cover the maturity space in a more coherent way. The current formulation of the Tiers is thin and has not been picked up by industry, indicating a lack of value. Internally for our uses, the concept of "maturity" is being handled by the CMMI Maturity Levels. With the introduction of NISTIR 8286 and the ID.SC category, it seems that many of the questions that would be posed through the Tiers, are covered elsewhere. To reduce confusion, removing the Tiers and pointing to more relevant documentation may be the best course of action.
2) *Streamline the Core* – The Core, in its current state is very useful because it attempts to define the "what" of cybersecurity risk management. Version 1.1 of the CSF moved more towards that concept by removing adverbs such as "continually" and "frequently" from subcategories. Continuing to focus on the "what" will improve the Core. As such, removing the "Improvements" categories from the Respond and Recover, would eliminate the "how" to do cybersecurity from the Core. These categories are notoriously difficult to score and harmonize with the other categories within their respective functions
3) *Revamp Recover* – The Recover function is light on content and is an important part of the cybersecurity risk management process. While many of the components which could be considered in Recover are present in other functions, the function itself needs a revisit.

Concepts from NIST SP 800-184: Guide to Cybersecurity Event Recovery could be used for this endeavor.

5. **Additional ways in which NIST could improve the Cybersecurity Framework, including resources supporting the Framework, or otherwise make it more useful.**

   ISO/IEC 27110 provides a guideline for creating cybersecurity frameworks. The NIST CSF meets the guidelines established in ISO/IEC 27110. Therefore, NIST could explicitly recognize the alignment and utilize a standards-based process to creating the next iteration of the CSF. This approach would not only continue to provide a common language and process for creating cybersecurity frameworks, it would also explicitly continue NIST's commitment to international alignment.

   **Relationship of the NIST Cybersecurity Framework to other Resources**

6. **If and how your organization uses other NIST risk management resources in conjunction with the NIST Cybersecurity Framework or separately, describe commonalities, conflicts, and suggestions for improving alignment or integration. These resources include:**

   - **Risk management resources such as the NIST Risk Management Framework, the NIST Privacy Framework, and NISTIR 8286 (Integrating Cybersecurity and Enterprise Risk Management).**
   - **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.**

   STLLC uses the NICE Workforce Framework for Cybersecurity (NICE Framework). Our tools provide interactive views into the large dataset of the NICE Framework [3]. Currently, we only have the NICE Framework in our tool set. We intend to broaden our tool scope in the near future. However, in our consulting, we leverage the NICE Framework and the CSF together as part of a holistic view into a cybersecurity risk management program.

   [3] https://www.yourcyberwork.com/tools

7. **If and how your organization uses non-NIST voluntary, consensus frameworks or approaches in conjunction with the NIST Cybersecurity Framework, describe commonalities, conflicts, and suggestions for improving alignment or integration. These include but are not limited to international approaches like the ISO/IEC 27000-series, including ISO/IEC TS 27110.**

   STLCC does not use these resources at this time.

8. **If and how your organization has used the content and approach contained in the NIST Cybersecurity Framework either in establishing or responding to a policy or requirement, including outside of the United States.**

STLCC does not have a comment on this topic at this time.

9. **References that should be considered for inclusion within NIST's Online Informative References Program. This is an effort to define standardized relationships between elements of documents, products, and services and various NIST documents such as the NIST Cybersecurity Framework, NIST Privacy Framework, and NIST Special Publication 800-53.**

   STLCC does not have a comment on this topic at this time. In the future we plan on producing OLIR content.

**Cybersecurity Supply Chain Risk Management**

10. **Approaches, tools, standards, guidelines, or other resources that your organization uses today to manage cybersecurity-related risks to supply chains.**

    STLCC does not have a comment on this topic at this time.

11. **The greatest challenges your organization faces related to the cybersecurity aspects of supply chain risk management and potential gaps observed in existing cybersecurity supply chain risk management guidance and resources. Please describe how they apply to information and communications technology, operational technology, IoT, and industrial IoT.**

    STLCC does not have a comment on this topic at this time.

12. **Whether and how cybersecurity supply chain risk management considerations might be further integrated into the NIST Cybersecurity Framework.**

    From a conceptual perspective, STLCC proposes two mutually exclusive suggestions. Statements 12 and 13 have the same response.

    1) *Strengthen the ID.SC category and do not publish a standalone Cybersecurity Supply Chain framework* – This category could be revamped to streamline language of current subcategories and add new ones. The current subcategories in ID.SC are lengthy and could be trimmed to be more in line with the rest of the outcome statements.
    2) *Remove the ID.SC category and publish a standalone Cybersecurity Supply Chain framework* – This approach allows the CSF to maintain focus on the organizational aspects of cybersecurity while allowing a standalone document to handle the intricacies of the cybersecurity supply chain. If NIST chooses to publish a standalone document, it would be greatly beneficial to industry if clear guidance on how to use that document in conjunction with other documents is also published. Without this guidance, yet another framework will only add confusion to an already difficult set of policies, documents, and resources.

13. **Whether and how a separate framework to address cybersecurity risks in supply chains might be valuable and developed.**

From a conceptual perspective, STLCC proposes two mutually exclusive suggestions. Statements 12 and 13 have the same response.

1) Strengthen the ID.SC category and do not publish a standalone framework – This category could be revamped to streamline language of current subcategories and add new ones. The current subcategories in ID.SC are lengthy and could be trimmed to be more in line with the rest of the outcome statements.
2) Remove ID.SC and publish a standalone Cybersecurity Supply Chain Framework – This approach allows the CSF to maintain focus on the organizational aspects of cybersecurity while allowing a standalone document to handle the intricacies of the cybersecurity supply chain. If NIST chooses to publish a standalone document, it would be greatly beneficial to industry if clear guidance on how to use that document in conjunction with other documents is also published. Without this guidance, yet another framework will only add confusion to an already difficult set of policies, documents, and resources.

If you have any questions related to our letter or would like to discuss further please email seemlesstransitionllc@gmail.com.

Sincerely,

Matthew Smith,
CEO and Founder, Seemless Transition LLC