NIPPON TELEGRAPH AND TELEPHONE CORPORATION

November 4, 2023

Submitted via email to cyberframework@nist.gov

National Institute of Standards and Technology
United States Department of Commerce
100 Bureau Drive
Gaithersburg, MD 20899

Re: NTT's comments in response to the public draft of the NIST Cybersecurity Framework 2.0

NTT appreciates the opportunity to provide comments to the National Institute of Standard and Technology (NIST) regarding the public draft of the NIST Cybersecurity Framework (CSF) 2.0. As an international partner, NTT has been engaged in NIST's CSF efforts for many years, working to provide constructive feedback and comments, actively participating in stakeholders' discussions, and helping to shape the CSF to be a truly global consensus-based framework. NTT continues to contribute to further evolution of the CSF through every opportunity throughout the revision process.

NTT is broadly supportive of the overall direction of the changes outlined in the draft. NTT is pleased to see that the key attributes of the CSF – flexible, high-level, technology neutral, common language, risk-based, outcome-based, and consensus-based framework – are well preserved in the draft. These attributes are the core values of the CSF that framework users have benefited from for many years and should be maintained throughout the evolution of the framework regardless of its version.

For further improvement of the CSF, NTT would like to offer the comments below:

- Cybersecurity Supply Chain Risk Management (C-SCRM)

C-SCRM should be taken into consideration holistically in an organization's cybersecurity risk management process, and therefore it should be addressed throughout the CSF Core across Functions. With that sense, it would be

reasonable that the draft takes hybrid approach with C-SCRM-specific Category (GV.SC) under the Govern Function as well as the Categories and Subcategories within the other five Functions which can be selected as appropriate based on actions taken with GV.SC. Since the Govern Function is closely related to the other five Functions as an overarching Function, it would make sense the C-SCRM-specific outcomes are placed under the Govern Function, as they are also closely related to the other Functions. C-SCRM Category (GV.SC) would well formalize key outcomes for organizations to consider managing cybersecurity risk in supply chain.

While in-depth information on C-SCRM itself can be discussed in external resources, such as SP 800-161r1, the draft could address more on how an organization can apply and leverage the CSF for its cybersecurity risk management and governance in their entire supply chain. For instance, basic concepts or key considerations behind outcomes outlined in GV.SC could be discussed more clearly in the section 3.5 as we believe that they are the foundation of organization's risk management process for supply chain. The section could also provide high-level guidance or examples on the steps for establishing C-SCRM program based on the basic concept. This is partially mentioned in the section of the draft but it could be further improved as is done in the section 3.1 for how to use the Profile. In addition, it would be crucial to expand supplemental resources, such as use cases, practices, and starter guides, to help organizations understand, prioritize, and implement the C-SCRM program with the CSF accordingly. It is ideal that organizations throughout the supply chain use the same framework to better manage and communicate with their cybersecurity risk within the ecosystem, and having more resources would be especially helpful for small and medium-sized organizations which may not have sufficient cyber resources but need to be secured as part of entire supply chain. As supply chain issues are broad and complicated, which cannot be solved in a single or universal way, it may also be important that stakeholders share their practices, learn each other from them, and improve their own C-SCRM program continuously. Since a number of C-SCRM documents already exist, the resources should be focused on how the CSF can be leveraged for organizations' C-SCRM.

- Guidance on CSF Implementation

To increase the use of the CSF globally, there needs to be support to help organizations implement the framework allowing the transition from high-level concept into practical operations. While matured enterprises may not necessarily need detailed guidance, it would be helpful to especially small and medium-sized organizations which may not have a defined cybersecurity risk management program. Supplemental resources, including guidance, use cases, practices, and templates, should be expanded, and maintained dynamically and separately from the CSF itself. This is a community-wide effort – it should be led by NIST, but stakeholders can also develop and share useful resources. NTT has contributed to providing our use cases as success stories along with practical tools and templates, and we will continue to cooperate with NIST and community in providing our practices as well as lessons learned from applying CSF 2.0 to our internal management.

One of the necessary resources would be the guidance to help smooth transition from CSF 1.1 to 2.0 which includes considering environments where both CSF 1.1 and 2.0 are in place. Since there are a large number of organizations that have already adopted the CSF 1.1, making the transition easy and cost-effective is the key to increase the use of latest version building on their existing program. Organizations may have also adopted 1.1 fully and lack this maturity in other areas of their security functions. Therefore, the guidance could include a comparison chart showing Categories and Subcategories in version 1.1 and 2.0 as well as supplemental information ensuring backward compatibility as much as possible.

- Implementation Examples

NTT is supportive of the proposal to introduce the Implementation Examples as an additional column in Framework Core. They will help close the gap between Subcategories, which are intentionally abstract, and the Informative References, which are more specific such as security controls. It is also reasonable that they are maintained separately in an online format to allow more frequent updates. Given the broad applicability of the CSF, it would be preferable to keep developing further examples. While the Implementation Examples are beneficial to the users, NIST should clearly state that they are just examples and not intended to be used as a set of mandatory requirements or a checklist that organizations should comply with. The level of abstraction of the examples could be appropriate overall. However, in several places, examples may need more clarity to explain what exactly the Subcategory means, as the level of description of the Subcategory and its Implementation Examples are the same (e.g., GV.SC-01 and its EX1).

- Framework Tiers

The section 3.3 discusses how to use Framework Tier but it may need further clarification of the scope and applicability of the Tier. We understand that the Tier is originally designed to be used to determine an organization's current and desired state in its cybersecurity risk management and governance as a whole and have a common understanding of the state within the organization. Therefore, although the Tier selection may affect creating and updating the Profiles, it is not intended to be applied directly to Subcategories. While it would be acceptable that the Tier can be used in many different ways by different organizations, its fundamental concept as mentioned above could be more clearly explained at the beginning of the section.

NTT appreciates the opportunity to provide feedback and comments to the draft and participate in this revision process. NTT welcomes the opportunity to answer any questions regarding this document and have follow up discussions. NTT looks forward to continuing to collaborate with NIST and engage in developing and implementing CSF 2.0 as a global consensus-based framework.

Sincerely Yours,

Shinichi Yokohama
Group CISO, NTT Corporation