NIPPON TELEGRAPH AND TELEPHONE CORPORATION

March 3, 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 NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework

1. Introduction

NTT appreciates the opportunity to provide comments to the National Institute of Standard and Technology (NIST) regarding the "NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework". As an international partner, NTT has been engaged in NIST's Cybersecurity Framework (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 global consensus-based framework. NTT continues to contribute to further evolution of the CSF through every opportunity throughout the revision process.

This document is organized as follows. Section 2 presents NTT's use of the CSF for group-wide cybersecurity risk management and governance. Then, section 3 discusses specific comments to the Concept Paper that may be worth considering in developing CSF 2.0.

2. NTT's Use of the NIST Cybersecurity Framework

2.1. NTT's On-going Success Story on Group-wide Cybersecurity Risk Management and Governance based on the CSF

- NTT as a diversified organization

NTT is a global technology and business solutions provider which consists of approximately 900 different operating companies (OpCos) with more than 300 thousand employees across the globe. It has been expanding its business

portfolio from the telecommunication business into integrated ICT solutions, real estate, energy, medical and health care, finance, etc., and OpCos are diversified in their service offerings, geographic locations and business models. Each organization has its own threats and risks, and thus its risk management process, cybersecurity program, and priority are all different from each other.

- Fundamental review of NTT's security policy and standards

Based on such corporate background as well as a shift to remote-based business environment under COVID-19, NTT conducted a fundamental review of its group-wide internal security policy and standards in 2021. The existing security policy and standards had been revised and updated piece by piece over the years, and had become an unwieldy set of documents. Therefore, NTT decided to take a fundamental approach to re-develop a whole structure and established brand new policy and standards last year. In the new policy and standards, the NIST CSF is positioned as a key component to enable risk-based management across the entire NTT group, and organizations can benefit from key attributes of the CSF including flexibility and applicability to any types of organizations and common language feature in cybersecurity risk management.

- Group-wide cybersecurity risk management and governance based on the CSF

Along with the new security policy and standards, NTT also initiated a group-wide cybersecurity risk management and governance based on the CSF. Considering the diversified environment of NTT group, the parent company NTT Holdings does not take genuinely centralized governance approach but rather aim for a federated governance or a form of aligned independence. NTT judged the CSF, given its flexibility, is a useful tool for its group-wide cybersecurity risk management. Specifically, Holdings requires each OpCo to conduct risk-based management using the CSF at a company scale allowing a certain extent of flexibility while ensuring group-wide security policy and standards. Then, Holdings communicates with OpCos using the results of the processes, consolidates all of those, and conducts risk management at a whole group scale. While the CSF is often adopted in a single entity, NTT's use case shows how the CSF can be used for multi-entity group risk management. The details are explained in following paragraphs.

- How it works

The group policy and standards require OpCos to conduct each step of cybersecurity program illustrated in section 3.2 of the CSF at least once a year, as risk management at a company scale. Each OpCo creates a current and target Profile and conducts risk assessment (using a risk heat map). Then, an action plan is developed and approved through communications among stakeholders including senior executives. One of the aims to use the CSF is to have common understanding between CISO and information security practitioners as well as CISO and senior executives at individual OpCo. Since this is risk management process at a macro level, it puts emphasis on having broad and comprehensive perspective rather than sticking too much to the details for preciseness so that it can

better identify higher risks and prioritize the actions. The result is used as input to the company-wide business risk management processes.

Holdings also takes the same steps to develop an action plan as a group-wide cybersecurity initiative through creating Profiles and conducting risk assessments from the Holdings perspective at the entire group scale. This is done at least once a year, but the risks are reviewed on a quarterly basis to address changes in risk environment, taking into consideration cyber incidents that have occurred within the group and the threat landscape observed within and outside the group.

In addition, Profiles, risk heat maps, and action plans developed by OpCos are provided to Holdings and used as a common language for risk communications between Holdings and OpCos. Through this process, Holdings consolidates risk information shared by OpCos and understands group-wide risks and actions undertaken by NTT OpCos. Then, Holdings validates whether they are aligned with its own Profiles and risk heat map as a whole group view and modify the group-wide action plan if necessary. The result of this Holdings' process is shared with OpCos as group-wide risk understanding and action plan, and used as input to risk management process of each OpCo. The result is also shared with group-wide business risk management at Holdings.

Note that the Profile and risk heat map are based on self-assessments and never used to compare maturity among participating OpCos. They are instead used for Holdings to understand what kinds of risks are considered serious in each OpCo and how each OpCo addresses those risks, and ensure alignment with risks and action plans identified by Holdings.

- Implementation guidance

In order to empower OpCos to conduct risk management using the CSF, Holdings provides comprehensive implementation guidance. It includes step-by-step instructions with Holdings' use case, examples of measurements and assessments, and templates of the Profile and risk heat map. OpCos are allowed to customize the way to adjust it to their existing management as long as group policy and standards are maintained. The implementation examples are discussed in detail in the next subsection. In addition to the guidance, Holdings holds working-level meeting and one-on-one CISO meetings with each OpCo to support its risk management process. It is important that both Holdings and OpCos sit side-by-side and share lessons learned and best practices with each other to build foundational capability as a group.

- Management implications

NTT group sets the following three key overarching considerations in cybersecurity risk management based on the CSF so that both senior executives and information security practitioners can share a common understanding.

- This new management process helps us reframe organization's existing risk management process (such as identifying risks and implementing/prioritizing actions) from the perspective of the CSF as a common framework across the group.
- Since the risk management process is conducted based on both "situational awareness" (fact) and "business strategy" (will), its outcome is consensus-based and not necessarily intended to be completely accurate.
- The information generated through the risk management process is not used to compare maturity with other organizations but instead is used to compare views between senior executives and practitioners and have common understanding between them.

2.2. Implementation Examples: Profile and Measurement

NTT developed its own Profile template to create current and target Profiles (see appendix). It introduces the original four-point scale to be applied to Subcategories, as shown below, and generates radar charts in the same way as other publicly available tools. The definition of the scale is developed based on the concept described in *Risk Management Process* part of Tier definitions in the CSF.

- Level 1: a relevant organizational rule is not defined, but a subcategory (outcome) is implemented partially.
- Level 2: a relevant organizational rule is defined, and a subcategory (outcome) is implemented based on it.
- Level 3: a relevant organizational rule requiring continuous improvement is defined, and a subcategory (outcome) is implemented based on it.
- Level 4: a relevant organizational rule requiring continuous improvement and timely adoption of the latest information is defined, and a subcategory (outcome) is implemented based on it.

The level is determined by the information security team in each OpCo based on the perspective derived from their daily cybersecurity operations, as it would not be feasible to automatically calculate the level based on the data collected from various security solutions implemented throughout the organization. The definition above is an example provided by Holdings and can be customized by OpCos so that it can better fit with risk management process of each organization.

The "relevant organizational rule" in the definition means that rules, terms, procedures, processes, etc. are clearly defined in OpCos based on the group-wide security policy and standards. Since this is intended to be used to measure the degree of maturity of a cybersecurity program in the entire organization as part of cybersecurity governance, the definition above focuses on whether and how in depth relevant organizational rules are defined. For instance, if an appropriate security measure is voluntarily implemented in a limited scope of an organization without clearly defined organizational rules, it would not be taken into account for the evaluation. In contrast, if an OpCo's specific rule, which is built on group-wide security policies and standards based on its own risk-based

management, requires higher degree of security measures and they are implemented properly, a higher value can be applied.

The four-point scale also defines the intermediate values between levels, as there could be cases where a relevant organizational rule exists, but requirements and/or scope of the rule are insufficient; or a relevant organizational rule is well defined, but it is not implemented in a subset of systems and/or subordinate organizations. Such cases can be represented by the intermediate value such as level 1.5, 2.5 or 3.5. Since this is intended to be used to have broad and comprehensive view of the organization, values at more granular level (e.g. level 1.1 or 1.2) are not defined. For the same reason, OpCos can apply a defined value as complete if more than 80% of subordinate organizations meet the requirement.

The concept and examples explained above are included in the guidance that Holdings provides for OpCos. It also includes a mapping between Subcategories in the CSF Core and related sections of NTT group-wide policy and standards as well as suggested values to be applied to each Subcategory when relevant group-wide policy and standards are fully implemented. Based on NTT's experience in developing the Profile template, it would be helpful for those new to the CSF to provide examples of the Profile template along with scale to measure the Core, in Function, Category, and Subcategory level, for creating Profiles, and key considerations in implementation. In addition, if it would be reasonable to use the Tiers concept to measure the Core for creating the Profile, it could be useful that the CSF or supplemental documents illustrate how the state of Tier 1 to 4 corresponding to each Subcategory can be represented/described.

Note again that creating the Profile is for self-assessment purpose, and it is not used to compare maturity among organizations but used for communications between Holdings and OpCos for mutual understanding. Since there is no single approach to measure and assess the CSF, OpCos are allowed to customize the Profile template including the scale described above so that flexibility in implementation can be maintained. It would also be important to educate stakeholders including senior executives about implications of measurement as well as basic concept of cybersecurity risk-based management.

3. Specific Comments

NTT supports the basic idea on the CSF update described in the Concept Paper, including maintaining applicability, flexibility, simplicity, technology neutrality, and consensus-based framework; increasing international engagement; improving mappings; providing more guidance and examples; and increasing usability. The rest of this section describes specific comments to the Concept Paper except ones presented in the previous section.

- Add implementation examples for CSF Subcategories

NTT suggests that the implementation examples are documented in other resource and mapped with the CSF by informative reference in the same way as NIST SP 800-53, which is a more implementation-oriented resource, mapped with the CSF. If those examples are added as a column included in the CSF Core, they could be used incorrectly as a check list for compliance. If the examples only include general explanations without mentioning specific implementations, they could be added as a column.

- Add a new Govern Function

Because processes related to cybersecurity governance can be the foundation of other activities, it would be understandable that Business Environment (ID.BE), Governance (ID.GV), and Risk Management Strategy (ID.RM) are put together and placed as a set of Subcategories in the Core. One thing to note is that there may be still room for consideration on how to maintain the backward compatibility in addressing suggested changes.

- Expand coverage of supply chain

As suggested in the Concept Paper, cybersecurity supply chain risk management (C-SCRM) outcomes could be further integrated throughout the CSF Core across Functions, since such outcomes exist not only in the Identify Function, which remains important part of C-SCRM, but also other Functions.

In C-SCRM, it is important that organizations identify, assess, and manage both first- and third-party risks. It would not be simple to cover all dependent organizations in the supply chain for cybersecurity risk management based on the CSF, compared with applying it in limited and clearly defined scope of entities. In that case, it would be crucial to emphasize strong collaboration among those organizations. In addition, an organization may also need to collaborate with other external parties, which are not necessarily in the supply chain, in case of emergency. In that sense, a collaborative element could be emphasized more as desired outcome from the perspective of Identify, Detect, and Response. Furthermore, since third parties may include various types of organizations such as outsourcing contractors for operations and software development, cloud service providers, infrastructure providers, product vendors, etc., differences in their desired outcomes may need to be considered.

With regard to the treatment of secure software development, NIST's Secure Software Development Framework (SSDF) could be mapped with the CSF through informative reference as the SSDF includes a number of specific implementation examples.

- Provide additional guidance on Framework Implementation Tiers

As presented in the previous section, NTT technically does not use the Tiers themselves for creating Profiles, as the CSF does not clearly explain how the Tiers concept can be used to measure the CSF Core in Subcategory level. While NTT supports the idea to better clarify the scope and applicability of the Tiers, they should not be used for

external communications as risk management process using the CSF is based on self-assessment.

- Other comments

If a risk heat map, a graphical representation of the likelihood and impact of cybersecurity events, is useful to represent the results of a risk assessment, it could be mentioned in the section 3.2 of the CSF as an example. In addition, providing a risk heat map template would help those new to the CSF conduct a risk assessment.

4. Conclusion

NTT appreciates the opportunity to provide feedback and comments to the Concept Paper 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
CISO, EVP of Security and Trust Office
NTT Corporation

Appendix:

- NTT_Profile_Template.xlsx
- NTT_Profile_Template_provisional-translation.xlsx