Before the
Department of Commerce
and the
National Institute of Standards and Technology

In the Matter of	)	
	)	
Evaluating and Improving	)	Docket No. 220210-0045
NIST Cybersecurity Resources:	)	
The Cybersecurity Framework and	)	
Cybersecurity Supply Chain Risk Management	)	
	)	

Response of
Nippon Telegraph and Telephone Corporation (NTT)
to Request for Information

Shinichi Yokohama
CISO, SVP of Security and Trust Office
NTT Corporation
Otemachi First Square East Tower, 1-5-1
Otemachi, Chiyoda-ku, Tokyo 100-8116
Japan

April 25, 2022

1. Introduction

NTT appreciates the opportunity to provide comments to the National Institute of Standards and Technology (NIST) regarding the Request for Information (RFI) on "Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management". NTT has been engaged with NIST in developing and implementing the Cybersecurity Framework (CSF) for many years, and it continues to contribute to further evolution of the framework through comments on the RFI and following discussions throughout the revision process.

2. NTT's Use of the NIST Cybersecurity Framework

2.1. Use Cases in the Past

A major advantage of the CSF is that it provides a common language and systematic methodology for managing cybersecurity risk. As a global technology and business solutions provider, NTT consists of about 900 different operating companies. These companies are very diversified in their service offerings, geographic locations, and business models. The CSF fits very well for providing a common language to this diversified group of companies. In early stage of NTT's adoption, it used the "Core" part of the CSF as a "common language" to bridge different units within NTT. Later, as the number of people who are familiar with the CSF increased, several of its operating companies started to use it as a risk management tool. In any case, its use cases have been "partial use" of the CSF by utilizing its versatility of taxonomy and a risk management approach.

2.2. On-going Use Cases

In the summer of 2021, NTT started an effort to review its group-wide internal security policy and standards. Prevalence of remote work under COVID-19 was one of major reasons which triggered this fundamental review. The existing security policy and standards have been revised and updated piece by piece over the years, and had become an unwieldy set of documents. NTT decided a greenfield approach to re-develop the new security policy and standards, and decided to embed the NIST CSF as a key component to enable risk-based management across the entire NTT group. Since the CSF defines the Core, Tier, and Profile in a conceptual and structured manner, it is quite useful as an international common language across the entire NTT group.

As another example, at a macro level, the parent company NTT Holdings conducts standardized security program management activities across constituent NTT companies using a risk-based approach based on the CSF. Comprehensive security controls in the Core with the Functions, Categories, and Subcategories help NTT Holdings visualize prioritized security enhancement

initiatives, and identify areas of improvement.

These efforts are still on-going, and the information that NTT provides in the following sections is generated through its experience in these on-going efforts. It is categorized into two types. First, Section 3 presents NTT's thoughts on overall CSF revision. Second, Section 4 presents specific recommendations that may be worth considering while revising the CSF 1.1 into the CSF 2.0.

3. Overall Comments to the CSF Revision Process

NTT recommends three principles for the CSF revision.

First, NTT hopes the CSF becomes truly globally common framework. NTT applauds NIST's effort so far to position the CSF as a global framework, but there is still a way to go. This CSF revision process is a good opportunity to advance this objective, and NTT encourages NIST to reach out to international stakeholders as much as possible so that their opinions and voices are reflected, and give them a strong stake in the outcome.

Second, NTT recommends NIST continues to position the CSF as a tool that entities use voluntarily for their own risk management based on individual tolerance to risk. Under an intensifying threat environment, an increased number of governments are starting to adapt regulatory approaches to enforce cybersecurity. Therefore, it is important that we have a voluntary framework that is jointly developed by a cross-section of global stakeholders from both industry and government. The regulatory approach each government takes is up to the individual government and relevant agencies, but the NIST CSF should remain as a voluntary tool for risk-based management of cybersecurity.

Third, there are several major changes and shifts in the threat environment and a continuous evolution of digital technology since 2018 when the CSF 1.1 was finalized. NTT hopes these major shifts and changes are addressed in the upcoming revision process. Examples of such major shifts and changes are: global spread of remote-based working environment, increased digital connectivity across entities, increased inter-dependency across entities and sectors, availability of advanced network technologies (such as 5G), and advancement in digital technologies (such as encryption). Addressing these does not require that the NIST CSF should have solutions to all of these issues. Rather, by addressing these issues in the revision process, NTT would hope for a more robust process and a more engaged set of global participants.

4. Specific Comments based on the RFI

In this section, NTT provides specific comments along with three buckets of questions in the RFI.

4.1. About the Use of CSF 1.1

- **Practical Usage for Beginners**

Looking at recent challenges in cyberspace, it is expected that the CSF will be more widely used by small and medium-sized businesses which may not have a defined cybersecurity risk management program, in addition to large enterprises like NTT that have already been utilizing it, to enhance their cybersecurity capabilities. While it is reasonable that the CSF is kept concise and high level for universal use, those new to the CSF may have some difficulty conceptualizing a concrete implementation. Given that the CSF is often the first document referenced regarding cybersecurity risk management in many organizations, supplemental information regarding implementation details could be added to 3.2. *Establishing or Implementing a Cybersecurity Program*. Such consideration for newer practitioners may help in expanding the adoption of the CSF in organizations of all sizes sectors and thus facilitate a more secure cyberspace.

For instance, in the seven steps illustrated in subsection 3.2, the resulting output of a step may not necessarily become an input to the subsequent step (e.g. from Step 3 (Create a Current Profile) to Step 4 (Conduct a Risk Assessment), and from Step 4 to Step 5 (Create a Target Profile)), which may cause confusion for newer practitioners. The purpose of each step and relationship among steps could be explained in more detail by, for example, categorizing or labeling steps as several phases, or referring/mapping steps to the corresponding processes of other risk management frameworks. It could also be beneficial to newer practitioners to provide external resources for practical examples of a risk assessment methodology and sample formats of the Profile as supplemental information. Having said that, NTT understands the CSF does not define such specific formats to keep the framework flexible and generic.

- **Refinement of Security Controls in the Framework Core**

Some of descriptions in the Subcategories in the Core can be reviewed and refined to make them more precise and actionable.

Remote Access:

Although PR.AC-3 in the Core speaks to managing remote access, in light of the large number of people currently working remotely, it could be clarified to include a wider assortment of decentralized communication strategies in a remote working environment. For example, a

user in a home environment directly connecting to a cloud service from a work laptop, without utilizing a centralized corporate VPN, is a growing trend. The direct communication between the user and the cloud service should also be managed, to ensure that policies are properly being followed and to prevent data leakage.

Security Control Validation:
Although PR.IP-7 and PR.IP-8 speak to improving protection processes and sharing protection effectiveness, explicitly stating that the strength and effectiveness of security controls must be validated on a regular basis may help to clarify PR.IP-8. Although it may be implied, sharing the effectiveness may be based on assessments that are done at one point in time, or as a result of an initial evaluation of a solution, tool, setting or process. Performing ongoing verification of security controls is a fundamental security activity that should be added.

Identifying Redundant System:
Unnecessary system duplication happens frequently. For example, a company may host multiple webs applications on multiple platforms and neglects to consider if those web applications could be consolidated. Continual growth without considering if assets can be consolidated can make system management unnecessarily complicated and continuously expands the attack surface, and thus increases cybersecurity risk. A process to identify redundant or unneeded systems on an ongoing basis can be added to PROTECT (PR) in the Core as a useful activity for nearly all organizations.

4.2. About Relationship of the NIST Cybersecurity Framework to Other Risk Management Resources

- **Alignment of the NIST Cybersecurity Framework with the ISO/IEC 27000 Series**

Improving alignment of the CSF with ISO/IEC 27000 series may increase adoption of the CSF globally, especially in Japan, where numerous organizations utilize ISO resources in cybersecurity management.

The Core and ISO/IEC 27001 Annex A:
Since each Subcategory in the Core provides informative reference to security controls defined in ISO/IEC 27001 Annex A, it is useful in comparing controls between the ISO and CSF.

Risk Management Process in the Tier and ISO 31000:
Although the Tier represents state (level) of risk management process in organizations, it does

not specify what this process is. To make this more understandable, it could clearly state that the process itself should be referred to other resources. Particularly in Japan, where many organizations use ISO resources, ISO 31000, which is referred to by ISO 27001, might be a familiar document as a typical example of risk management process. By stating that the Tier and ISO 31000 does not conflict but instead reinforce each other, those who are familiar with ISO/IEC series may easily note the alignment and complimentary nature of the two frameworks.

The Profile and PDCA in ISO/IEC 27001:
By stating that the Profile of the CSF can be used within Information Security Management Systems (ISMS), it could be helpful guidance for those more familiar with the ISO series. For instance, "Plan" in the PDCA cycle can be mapped to the step of creating a target profile, and "Check" in the PDCA cycle can be mapped to the step of creating a current profile and determining gaps between current and target profile.

- **Alignment of the NIST Cybersecurity Framework with the NIST Risk Management Framework**

NIST provides two major resources regarding risk management: the CSF and Risk Management Framework (RMF). There can be cases in which organizations have some difficulty in determining which to choose or how to use both properly. NTT understands that the CSF is a high-level framework that can be used broadly and generically, and therefore the most suitable document may depend on what they manage for what purpose. As each framework has its own scope and perspective, additional explanation on the relationship among related resources including the CSF and RMF, both in similarity and difference for a particular scope, typical use cases, etc. could be beneficial for users in choosing the best suited resource.

Reference to RMF:
While the RMF is well-mapped to other NIST resources including SP 800-53, SP 800-64, 800-161, and CSF, the CSF 1.1 does not provide reference to the RMF in the opposite direction. At a minimum this mapping could be added as a cross-reference between the CSF and RMF.

Guidance on the use of the CSF and RMF:
Additional guidance explaining a clear scope of both the CSF and RMF, relationships between the two and typical use cases could help users choose appropriate document or combination depending on their specific purpose. Furthermore, it would also be beneficial to provide a

structured view (e.g., system diagram) of the entirety of NIST resources surrounding and related to the CSF. Such a well-organized overview would greatly increase usefulness of not only the CSF but also other related resources.

4.3. About Cybersecurity Supply Chain Risk Management

As directed in E.O. 14028, ensuring cybersecurity in software supply chain is a crucial issue. While the supply chain perspective was added to the current version of the CSF, some additional focus on software could be added, based on existing initiatives in federal agencies, after the work is completed at those agencies.

Software Bill of Material (SBOM):

In software supply chain risk management, ongoing monitoring for known vulnerabilities is crucial. Software developed internally to a company often makes wide use of 3rd party libraries (both open and closed source). Those need to be inventoried (ideally in a central repository) and checked for known issues such as CVEs. This includes not only custom-built software but purchased hardware and software that itself will have embedded libraries. A list of embedded components and libraries within software, which is generally called Software Bill of Materials (SBOM), can be used for tracking and checking for vulnerabilities. This perspective could be added to IDENTIFY (ID) in the Core as a necessary security control.

Software Application Logs:

As PR.PT-1 in the Core states that audit/log records are determined, documented, implemented, and reviewed, it could be expanded to specify that software applications logs should be reviewed as well. This may already be implied, but software logs (for example, logs generated by a web application, not simply the web server logs) are often overlooked. In this way, many attacks against applications may be overlooked by SOC monitoring.

5. Conclusion

NTT would like to extend its gratitude for the opportunity to provide comments on the RFI and participate in this revision process. NTT is keen to continue to engage with NIST and contribute to further evolution of the Cybersecurity Framework. NTT also welcomes the opportunity to answer any questions regarding this document and looks forward to working closely with NIST.

Sincerely Yours,

Shinichi Yokohama
CISO, SVP of Security and Trust Office
NTT Corporation