NTT

NIPPON TELEGRAPH AND TELEPHONE CORPORATION
Otemachi First Square East Tower 1-5-1 Otemachi, Chiyoda-ku, Tokyo 100-8116 Japan

January 19, 2018

Comments on NIST Cybersecurity Framework Version 1.1 Draft 2

Dear Sir/Ma'am,

It is a great pleasure to have an opportunity to submit comments to the NIST Cybersecurity Framework Version1.1 Draft 2.

NTT has been participating in the multi-stakeholder process for developing the NIST Cybersecurity Framework, and comments in the attachment are based on such experience. They are structured with an Executive Summary followed by detailed full comments.

We commit to contribute to building global cyber resiliency. With such commitment, we hope to be a part of the processes and works going forward, i.e. organizations using and implementing the NIST Cybersecurity Framework as a cyber risk management tool.

Sincerely Yours,

Shinichi Yokohama
Head, Cyber Security Integration
NTT Corporation

Attachment

NTT

NIPPON TELEGRAPH AND TELEPHONE CORPORATION
Otemachi First Square East Tower 1-5-1 Otemachi, Chiyoda-ku, Tokyo 100-8116 Japan

Executive Summary

We should finalize documentation and move on to implementation.

Overall, the NIST Cybersecurity Framework (mentioned as CSF here after in this document) V1.1 Draft2 is well written. It covers and addresses all key issues, including "Measurement" and "Supply Chain Risk Management", in a comprehensive and balanced manner. We should finalize the documentation phase and move on to accelerating implementation of CSF V1.1.

We should not underestimate rigor and discipline required for CSF v1.1 implementation as a risk management tool.

The hallmark of CSF remains unchanged in V1.1 Draft2. There are three key attributes, i.e. 1) risk based management, 2) dynamic and continuous usage, 3) framework not standards. We should remind ourselves that it is not simple or easy to implement CSF V1.1 as a part of an organization's risk management. Full implementation of CSF V1.1 requires disciplined and rigorous risk management practice.

In implementation, we need to focus on using "Self-Assessment" to connect top management and front line operations.

We need to recognize that we are still at a very early stage of maturing our cyber security practice. For CSF V1.1 to be used with its full potential as a risk management framework for organizations, top management should be informed about the risks that arise from cyber in a measured way. Self-assessing the company's cyber security practice maturity level and progress along a time-line becomes useful here. We need to continue to emphasize the importance of "measurement" in a form of self-assessment.

We should accumulate use cases where measurement helps management decisions, and disseminate lessons learned, wisdom and knowledge from the use cases.

We should accumulate CSF V1.1 use cases where self-assessment is used for top management decisions. Specifically regarding the Roadmap, a combined effort of 4.6 "Governance and Enterprise Risk Management" and 4.9 "Measuring Cybersecurity" is recommended. We measure cybersecurity for the sake of sound decision making by management. We should avoid efforts to develop measurement approaches for the sake of measurement.

NTT

NIPPON TELEGRAPH AND TELEPHONE CORPORATION
Otemachi First Square East Tower 1-5-1 Otemachi, Chiyoda-ku, Tokyo 100-8116 Japan

Global participation is critical and we need to invite global partners, for example Japanese industry.

In CSF V1.1 implementation efforts, soliciting international participation continues to be critical. Attackers are diversified and global. We need to accumulate wisdom from diversified and global sources, i.e. use cases from international organizations. A strong candidate is Japan. Awareness of CSF is increasing, and foundation for international collaboration is being built in Japan.

NTT

NIPPON TELEGRAPH AND TELEPHONE CORPORATION
Otemachi First Square East Tower 1-5-1 Otemachi, Chiyoda-ku, Tokyo 100-8116 Japan

Comments to NIST Cybersecurity Framework v1.1 draft

We should finalize documentation and move on to implementation.

Overall, the NIST Cybersecurity Framework (mentioned as CSF here after in this document) V1.1 Draft2 is well written. It covers and addresses all key issues, including "Measurement" and "Supply Chain Risk Management", in a comprehensive and balanced manner. We should finalize the documentation phase and move on to accelerating implementation of CSF V1.1.

- Current draft positions "Measurement" as "self-assessment". This clarifies objectives of measurement and avoids risk that measurement is used for regulatory or un-voluntary purposes.
- "Supply Chain Risk Management" is clearly stated as an element of stakeholder communication. It ensures addressing SCRM when an organization uses CSF for its cyber security management.

We should not underestimate rigor and discipline required for CSF v1.1 implementation as a risk management tool.

The hallmark of CSF remains unchanged in V1.1 Draft2. There are three key attributes, i.e. 1) risk based management, 2) dynamic and continuous usage, 3) framework not standards. We should remind ourselves that it is not simple or easy to implement CSF V1.1 as a part of an organization's risk management. Full implementation of CSF V1.1 requires disciplined and rigorous risk management practice.

- People tend to pay attention to the CORE, in particular the 5 functions. However, the 5 functions are just a part of the approach proposed by CSF V1.1. There are 23 categories, 108 sub categories within the CORE. Moreover, there are Implementation Tiers and Profiles. Companies need to develop their own cyber security action plan by utilizing all of the CORE, Implementation Tiers and Profiles.
- Developing an action plan requires 6 steps described on pp19-20 of CSF v1.1. Once the action plan is developed, it is just a starting point. Executing the action plan is required (as Step 7 on p20 of CSF V1.1), and more importantly reviewing results and repeating Steps 1 to Step 7 is required. For companies to improve their cyber security along with their overall risk management practices, a dynamic and continuous usage of CSF V1.1 is essential.

NTT

NIPPON TELEGRAPH AND TELEPHONE CORPORATION
Otemachi First Square East Tower 1-5-1 Otemachi, Chiyoda-ku, Tokyo 100-8116 Japan

- CSF V1.1 does not tell companies what to do. The choice of Implementation Tier and design of Profiles are up to management decision. Achieving all 108 subcategories to the highest level is not "ideal but impossible" and "wrong" since it puts unnecessary pressure on the organization and can harm the cyber security of the organization. Pursing perfect benefits attackers. Smart and risk based usage is indispensable. It is a framework and not a standard.

In implementation, we need to focus on using "Self-Assessment" to connect top management and front line operation.

We need to recognize that we are still at a very early stage of maturing our cyber security practice. For CSF V1.1 to be used with its full potential as a risk management framework for organizations, top management should be informed about the risk that arise from cyber in a measured way. Self-assessing the company's cyber security practice maturity level and progress along a time-line becomes useful here. We need to continue to emphasize importance of "measurement" in a form of self-assessment.

- In many organizations, there is still a gap between top management and front line operation. Front line operation has difficulty in communicating its challenges, works and efforts, and achievements to top management. Since cyber risk management should be integrated into the overall risk management practice of an organization, top management wants to be informed for its decision makings along with its risk preference, but quite often such decision base is not provided.
- Using CSF V1.1 in a repetitive and dynamic way will remind organizations how critical and important measurement is for them to improve their cybersecurity. The last sentence of "4.0 Self-Assessing Cyber Security Risk with the Framework", i.e. "organizations are encouraged to innovate and customize how they incorporate measurements into their application of the Framework with appreciation of their usefulness and limitations" points out this challenge.

We should accumulate use cases where measurement can help management decisions, and disseminate lessons learned, wisdom and knowledge from the use cases.

We should accumulate CSF V1.1 use cases where self-assessment is used for top management decisions. Specifically regarding Roadmap, a combined effort of 4.6 "Governance and Enterprise Risk Management" and 4.9 "Measuring Cybersecurity" is recommended. We measure cybersecurity for the sake of sound decision making by management. We should avoid efforts to develop measurement approaches for the sake of measurement.

- Statement in 4.9 Measurement Cybersecurity is right - "This is an under-developed topic, one in which there is not even a standard taxonomy for terms such as "measurement" and "metrics". The development of reliable ways to measure risk and effectiveness would be a major advancement and contribution to the cybersecurity community."
- New cybersecurity measurement program suggested in 4.9 should emphasize supporting decision making by senior executives and oversight by boards of directors. For that purpose, use cases of CSF V1.1 in real business management will be the most useful source of wisdom. Combining 4.6 and 4.9 efforts will create lots of purposeful synergies, as opposed to each conducted individually.

Global participation is critical and we need to invite global partners, for example Japanese industry.

In CSF V1.1 implementation efforts, soliciting international participation continues to be critical. Attackers are diversified and global. We need to accumulate wisdom from diversified and global sources, i.e. use cases from international organizations. A strong candidate is Japan. Awareness of CSF is increasing, and foundation for international collaboration is being built in Japan.

- METI issued Version 2 of its "Cybersecurity Guideline for Top Management" in November 2017. This Version 2 clearly quotes five functions from NIST CSF, in particular DETECT, RESPOND and RECOVER. Since many corporate executives in Japan are aware of METI's Guideline, it is expected that awareness of NIST CSF among Japanese senior executives will increase.
- IPA (Information Promotion Agency: METI affiliated quasi-governmental agency) published a survey result among 755 Japanese companies in April 2017 about standards and guidelines referred or used by Japanese companies. The result shows 33% of Japanese companies "refer to or use" NIST CSF. To what extent they "refer to or use" CSF is unclear, and it may be fair to state that it is "awareness" not "reference or usage". Nonetheless, it is encouraging that many Japanese companies are already aware of NIST CSF.
- Japan Business Federation, the largest business association in Japan, published its third report on cyber security in December 2018. The report emphasizes industry driven approach, not government/regulation driven, for cyber security. With such emphasis, a foundation to adopt NIST CSF is being developed.
- "Cross Sector Forum" where 30+ Japanese blue chip companies from different industries have had multiple study-sessions on CSF. Since its foundation, they

have had study sessions on NIST CSF by inviting NIST staff to Tokyo. They are having additional working session to “digest” essence of CSF V1.1.