From: 横浜　信一 Shinichi Yokohama
Date: Thu, Mar 23, 2017 at 9:52 PM
Subject: Comments on draft Framework Version 1.1
To: cyberframework@nist.gov
Cc: chieko tokano

Dear Sir/Ma'am,

Attached please find NTT's comments on the draft.

Sincerely Yours,

Shinichi Yokohama
Head, Cyber Security Integration
NTT Corporation

[Attachment Copied Below]

NTT thinks that adding Supply Chain Risk Management (SCRM) to the Framework is great progress.

It would be helpful if a definition of "Supply Chain Risk" is elaborated in the final report.

It would be constructive for the conventional "buy-sell supply chain model" (where Company A buys a product/service from Company B, and that product/service is embedded in Company A's product/service) to be clearly addressed in SRCM.

What is unclear is whether the "operational supply chain model" addressed in draft Version 1.1 refers to a product/service by Company A that is operationally directly linked / connected to a product/service by Company B. For the customers, a combination of a product/service by Company A and a product/service by Company B is needed. One example of this model is where an ISP provides boradband internet access service to a home user and a home router company provides a router to the same home. The residential user needs both broadband internet access service and the home router to use the Internet.

This type of "operational supply chain model" will increase as more items include digital features and get connected to each other. Company A and Company B's relationship is not a buys-sell contractual arrangement, but rather they are equal partners. How Company A and Company B recognizes each other and jointly address collective cyber resiliency will increase in importance.

The changes, in particular adding SCRM, will have positive impacts on ecosystem cyber resiliency.

We are not sure to what extent metrics and measurements will enhance cybersecurity. We recognize the importance of metrics and measurements. However, the description in draft Version 1.1 is generic and it is not clear to us as to how to leverage those practically and operationally. It would be very helpful if we can see use cases.

NTT's usage of Version 1.0 is limited to Core as a common language within the organization. We assessed our cyber security capabilities along five Functions and twenty-two Categories. The proposed changes will not impact such usage, i.e. using Core as a common language. However, NTT is required to re-assess our capabilities along added categories, i.e. SCRM.

Some parts of NTT use ISO27001 as a security standard. The decision to use the Framework will depend on how easy it is to re-map ISO 27001 to the Framework. The draft Version 1.1 will not impact our usage decision much.

Is there a better label than "version 1.1" for this update? "The Industry Framework" is one idea. Thanks to the NIST's efforts, the Framework has created strong traction from multiple stakeholders. Although we may have multiple "versions" as we move forward, keeping the lable simple will make sense. Many recognize this is a living document. Also, many recognize this is owned and developed by the industries.

Are there any areas that should be removed from the Roadmap? - "International Aspects, Impacts and Alignment" is already addressed in Roadmap. Activities in the cybersecurity ecosystem reinforce the importance of international harmonization. Billions of new people will equip themselves with smart phones, and most of them are in emerging markets where interests by countries and governments are diverse. A much larger number of items ("things") are being connected to the INternet and the IoT society is becoming reality. Topics that will require international harmonization will increase in breadth, complexity and inter-dependency.

In Asia, each country is developing cyber security guidelines and interests in international harmonization are increasing, starting from governments but also among industries. In 2016, the Japanese government announced IoT cyber security guidelines and it hopes to harmonize it with international communities. At ASEAN-Japan Information Security Policy Meeting (October 2016), the eleven governments revised their cyber security guidelines for critical infrastructure industries. Among these countries, the Cybersecurity Framework is gaining traction as a reference point to develop national guidelines.

We recommend accelerating international harmonization efforts, in particular with Asian countries. We learned NIST has organized an international workshop in Europe and Middle East. Having a similar workshop in Asia in 2017 with international participants, both from public and private sectors, will have a strong impacts on expansion to Asia.

Increasing the number of people who can explain how to use the Framework is critical for successful adaptation of the Framework. This is in particular true for efforts outside the US. Efforts to increase "international friends and families" of the Framework is strongly encouraged.

Finally, given a significant workload to execute efforts around the Framework, it may be worth considering accept detailed staff to NIST from external entities including non-US.