NTT

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

February 2, 2016

Ms. Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive
Stop 8930
Gaithersburg, MD 20899

Re: Views on the Framework for Improving Critical Infrastructure Cybersecurity

Dear Diane:

NTT appreciates the opportunity to provide a view on the NIST Cybersecurity Framework. NTT has used the Framework on multiple occasions and across various venues, and would like to share our experience and what we learned from these cases. We also would like to provide some early thoughts about the future of the Framework.

NTT's experience informs us that the NIST Framework is very powerful and has benefits beyond its original design purpose. NTT has used it on multiple occasions, in particular for capability assessment and mapping purposes. Thse occasions cover both internal NTT applications as well as with other Japanese companies from multiple sectors. We have also used it in our publication to communicate to C-suites on cyber security risk management in a holistic manner. At all of these instances, we have found the Framework functions to be very effective as a common language for people with different backgrounds. (Exhibit 1) The following cases describe how NTT has been successful in adapting the Framework to our global service environment.

- Case 1: Service mapping to develop shared view on our collective capability
  NTT provides a comprehensive and compelling cyber security portfolio of services to our clients. However, we discovered that we lacked a consolidated view of our capabilities because we had grown rapidly through inorganic acquisitions over the last several years. In March 2015, NTT organized an internal workshop where professionals across operating companies got together and developed a service map

that shows our own collective capabilities. We used the five functions and the 22 categories of the NIST Framework as a common language for our discussions. (Exhibit 2)

The Framework allowed us to create a common view of our services and facilitated a strategic discussion around where we are strong and where we could benefit from further enhancements..

- Case 2: External communication of "full stack and full life-cycle" capability

  NTT is a unique ICT service provider that is ranked in the global top five both in network service and IT service with an operational footprint in more than 80 countries. As such, our value proposition to clients is an ability to provide security services in "full stack and full life-cycle". In communicating such a value proposition, we developed our own framework which is built around the NIST Framework's five primary functions or "life-cycle". (Exhibit 3)

  The Framework was also used to drive internal discussions.. For example, at our CISO Committee, we discussed how to enhance our internal protection capabilities using the Framework construct.

- Case 3: Collaborative action planning and implementation against Advance Persistent Threats (APT)

  When the CISO Committee discussed collaborative actions to protect ourselves against increasing APTs, we used the five functions of the NIST Framework to map required actions from both technological and organizational angles. (Exhibit 4)

  After agreement, actions were cascaded down to field operations. We found the Framework to be useful as a common language in executive-level discussions, field level operations, and importantly, communication between executives and the field.

- Case 4: Cross-sector discussion on NICE workforce development

  NTT convened a cross-sector forum among Japanese companies. Forty-plus companies from different sectors participated in this forum and discussed workforce development and information sharing. In our early discussion, we found profiles of required workforce are quite diverse and that a common understanding among participating companies is important. We used the NICE workforce framework, and worked to link the NICE profiles to the roles of IT organizations. In doing so, the NIST Framework was useful to ensure a shared

understanding of "bridging" the NICE profiles with IT organizational resources. (Exhibit 5)

- Case 5: C-suite communication of holistic cyber security approach
  NTT published a book in Japan in October 2015. It is targeted to business executives of Japanese corporations, and in particular business leaders and C-suite executives. Our message was simple, "Cyber security is not just an IT issue. It is a business issue." In explaining the principles and measures to be taken by C-suite executives, we again referenced the five key functions of the NIST Framework. (Exhibit 6)We found the Framework's five functions are easy to understand for non-technical business executives, and help them shape corporate actions to increase their cyber resiliency.

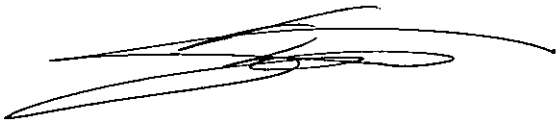
It is the view of NTT that currently offenders have structural advantages over defenders, and that "game change" efforts must happen so that offender advantages are minimized. (Exhibit 7) To make such "game change" happen, everybody's participation is needed, e.g. information sharing among user companies, robust security service by providers, etc. (Exhibit 8) We believe such "game change" is possible not by a single big invention but by a combination of physical technologies and social technologies. Talent plays a critical role here. International collaboration and co-working by all defenders is important for all of these three, e.g. physical technologies, social technologies and talent development. (Exhibit 9)

Our view is, in such context, that the NIST Framework should be much more aggressively promoted internationally. In promoting it internationally, NTT recommends NIST considers enhancing the Framework from its original intention, i.e. critical infrastructure protection. We share some ideas of such enhancement from four angles, 1) Scope of application, 2) Stakeholders to involve, 3) Vehicle for adaptation, 4) Governance. (Exhibit 10) Ideas described on Exhibit 10 are very preliminary, and should be positioned as the basis for starting the discussion. Our intention of Exhibit 10 is facilitating key issue identification rather than proposing concrete answers.

We have complete trust in the multi-stakeholder approach that NIST has undertaken. In fact, such an approach can be an integral part of "game change" innovation. With such confidence and trust, we are happy to continue to participate in this process, and in particular help to promote international alignment.

We welcome the opportunity to answer any questions regarding this document and thank you again for this opportunity.

Sincerely Yours,



Shinichi Yokohama
Head, Cyber Security Integration
NTT Corporation

Attachment: 160202 Exhibits to memo