



U.S. CHAMBER OF COMMERCE

May 25, 2018

Mr. Toshikazu Okuya
Director, Cybersecurity Division
Commerce and Information Policy Bureau
Ministry of Economy, Trade and Industry
1-3-1 Kasumigaseki
Chiyoda-ku, Tokyo 100-8901, Japan

Subject: Public Consultation on Japan's Draft Cyber/Physical Security Framework

Dear Mr. Okuya:

The U.S. Chamber of Commerce ("Chamber") is the world's largest business federation, representing the interests of more than three million businesses and organization of every size, sector, and region, including members supporting jobs for thousands of Japanese citizens. We are firm supporters of a productive U.S.-Japan relationship and our members are representative of the vital business community that contributes substantially to increasing jobs and growth in both Japan and the United States.

The Chamber and the U.S.-Japan Business Council ("USJBC") welcome the opportunity to respond to the Ministry of Economy, Trade and Industry's draft Cyber/Physical Security Framework ("Framework"). Overall, we support METI's efforts to establish a voluntary, risk-management based framework. We strongly believe that a multi-stakeholder approach to cybersecurity is the most effective way to encourage economic activity while ensuring security. While the Chamber and USJBC broadly support the draft Framework, we suggest below certain ways that it could be further strengthened or would benefit from further clarification.

One consideration relates to how small and medium sized enterprises ("SMEs") will utilize the framework. The level of detail in the proposed draft is high, making it less accessible for companies that do not have sophisticated internal cybersecurity capabilities. Many such companies will also outsource parts of security management to third parties. We encourage you to develop subsequent guidance which is more accessible for SMEs, as well as to provide greater clarity around their responsibilities when outsourcing cybersecurity functions to third parties.

Second, there is broad consensus in industry that a multi-stakeholder framework is a sound baseline for businesses' cyber practices, including internationally. The Chamber has communicated this in the U.S. context to consecutive Presidential administrations, and we maintain that such an approach is the cornerstone for managing enterprise cybersecurity risks and threats globally. Beyond the benefits that interoperability brings from a trade perspective, it ensures that companies can scale best-in-class cybersecurity practices across borders, raising overall levels of cybersecurity. While we applaud the discussion of international alignment in the draft Framework, we encourage you to develop a more detailed strategy for how the Ministry

Mr. Toshikazu Okuya
May 25, 2018
Page Two

will work with their international counterparts and industry to promote interoperability among cyber regulations.

Finally, we ask that coordination within the Japanese government on the Framework be prioritized. Too often companies face regulatory uncertainty around the world when different domestic agencies establish competing frameworks or regulatory schemes related to cybersecurity and the digital economy. While Japan has been a global leader in ensuring that companies do not face such uncertainties, we have noticed slightly different approaches in how METI and the Ministry of Communications are approaching industrial cybersecurity. Ensuring that the two are coordinated in their approaches will help to mitigate any risks or challenges to the ICT and cybersecurity industry's growth in Japan.

The Chamber values the considerable effort that METI has put forth to establish and update the framework, and appreciates the opportunity to offer our views. If you have any questions regarding our comments, or need more information, please do not hesitate to contact James Fatheree (jfatheree@uschamber.com) or Sean Heather (sheather@uschamber.com).

Sincerely,

James W Fatheree
Vice President
Asia

Sean Heather
Vice President
Center for Global Regulatory Cooperation