February 28, 2019

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 U.S. companies that have invested billions of dollars in Japan and support 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 our affiliated 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, and we very much appreciate the willingness of the Government of Japan to consult with industry throughout the drafting process.

As noted in our previous comments, we strongly believe that a multi-stakeholder approach to cybersecurity is the most effective way to encourage economic activity while ensuring security, and that effective cybersecurity is fundamental to the resiliency of digital infrastructure, digital trade, and the global value chain. While the Chamber and USJBC broadly support the draft Framework, we suggest below certain ways that it could be further strengthened:

1. The proposed Framework provides a comprehensive view of the technical considerations for developers in creating secure IoT or cyber/physical solutions. However, as we strongly believe that risk management is foundational to effective cybersecurity, there is a demonstrated need for policies to reflect risk-based approaches and prioritize implementation of risk management processes. Thus, we recommend that the Japanese government endeavor to employ and encourage enterprises to use risk-based approaches that rely on consensus-based standards and risk management best practices to identify and protect against cybersecurity risks to detect, respond to, and recover from cybersecurity events. To accomplish this, we believe that the Framework should focus on

the assessment and identification of risk, methods for minimizing risk, and the maturity of companies in implementing international best practices.

2. The Chamber and the USJBC also believe that privacy certification schemes play an important role in creating trust with consumers as they use and deploy IoT and cyber/physical systems. To this end, we hope that the framework can better promote a strong culture of protecting data, wherever it is stored, alongside the secure, technical solutions outlined in the framework.

3. There is broad consensus in industry that a multi-stakeholder framework is a sound baseline for businesses' cyber practices, including in the international realm. The Chamber has communicated this to consecutive U.S. 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 also 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 METI to develop a more detailed strategy for how the Ministry will work with their international counterparts and industry to promote interoperability among cyber regulations.

4. 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, the Ministry of Internal Affairs and Communications, and the National center of Incident readiness and Strategy for Cybersecurity are approaching industrial cybersecurity. Ensuring that the Government of Japan is coordinated in these approaches will help to mitigate any risks or challenges to the ICT and cybersecurity industry's growth, and help strengthen Japan's overall cyber resiliency.

The Chamber and USJBC value 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 the Chamber's Vice President for Asia and President of the USJBC, David Gossack (dgossack@uschamber.com), or the Senior Vice President of the Center for Global Regulatory Cooperation, Sean Heather (sheather@uschamber.com).