THE SPIRIT OF ENTERPRISE U.S. CHAMBER OF COMMERCE ®

USJAPAN BUSINESS COUNCIL

May 29, 2020

Mr. Toshikazu Okuya
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 the Draft of "IoT Security Safety 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 strong 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 IoT Security Safety Framework ("Framework"). Overall, we support METI's efforts to establish a voluntary, risk-management-based framework, and we appreciate the willingness of the Government of Japan to consult with industry throughout the drafting process. The Chamber believes that taking industry voice into consideration only strengthens the end result.

As noted in our previous comments to METI, 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—especially when considering IoT devices.

The Chamber and USJBC broadly support the draft Framework's goal of creating a basic common infrastructure to review the security and safety of IoT devices and systems. However, we suggest below certain ways that it could be further strengthened:

- **Continue to pursue a risk-based approach that fosters innovation**. The Chamber strongly believes that risk management is foundational to effective IoT security. As the Framework develops, we recommend continuing a risk-based approach that relies on best practices to identify and protect against threats to IoT Security. To accomplish this, we believe that the Framework should focus on the assessment and identification of risk and methods for minimizing risk. Such an approach will foster innovation and reward security and innovation since the Framework will be able to adapt to new technologies.

- **Align with existing international best practices.** The Chamber recommends that the Framework be based on industry-led international standards and frameworks. Private industry greatly benefits when governments incorporate existing foreign cybersecurity frameworks, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework or the International Organization /International Electrotechnical Commission ("ISO/IEC") 27001:2013, into any future policy enactments. The framework is largely a process—one designed to help organizations start a cybersecurity program or improve an existing one—and can be applied to IoT security as well. The framework features a number of industry-vetted actions that businesses can take to assess and strengthen their state of security over time. Additionally, NIST is developing "Recommendations for IoT Device Manufacturers," and recent drafts align with the risk-based measured approach for which the Chamber advocates. Other sources of existing cybersecurity frameworks and best practices include: NIST Framework for Improving Critical Infrastructure Cybersecurity; Council to Securing the Digital Economy C2 Consensus on IoT security core capabilities baseline; and NISTIR 8259.

- **Place an emphasis on capacity building and information sharing.** The Chamber encourages capacity-building and information sharing between the public and private sector. We believe that sharing information makes companies and government alike stronger while weakening adversaries and cyber bad actors. We recommend that METI include a section in any future drafts that encourages those in the IoT device atmosphere to report and share threat intelligence and known vulnerabilities that could strengthen the ecosystem’s defense against bad actors.

- **Provide clarity on the next steps of the Framework.** As currently written, the Chamber interpreted the Framework as voluntary guidance. Additional clarity on the next steps of the Framework—for example, if there will be legislation around the Framework—would be helpful as companies consider next steps.

The Chamber and USJBC value the considerable effort that METI has put forth to create the Framework and appreciates the opportunity to offer our views. Both the Chamber and USJBC value our ongoing close relationship with METI and look forward to future collaboration. If you have any questions regarding our comments, or need more information, please do not hesitate to contact Senior Vice President for International Regulatory Affairs, Sean Heather (sheather@uschamber.com) or Executive Director for Japan, Aiko Lane (alane@uschamber.com).