ITI Promoting Innovation Worldwide

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

Via Email: cybersec_comment@meti.go.jp

RE: ITI Comment Submission to METI Draft of IoT Security Safety Framework (SSF)

The Information Technology Industry Council (ITI), appreciates the opportunity to submit the following comments to Japan's Ministry of Economy, Trade and Industry (METI) on the draft IoT Security Safety Framework.

ITI is the premier advocate and thought leader in the United States and around the world for the information and communications technology (ICT) industry, and represents over 70 leading companies from across the ICT sector, including hardware, software, digital services, semiconductor, network equipment, cybersecurity and Internet companies. ITI promotes innovation worldwide and seeks policy solutions for the increasingly connected world powered by the continuous rise of emerging technologies such as Internet of Things (IoT). The growth of network-connected devices, systems, and services comprising IoT creates immense opportunities and benefits for our society. To reap the benefits of connected devices and to minimize the potentially significant risks posed by malicious actors seeking to exploit them, these devices need to be secure and resilient. Organizations and individuals increasingly face challenges in recognizing and understanding cybersecurity risk across the full range of today's internet-connected devices, and some policymakers are disproportionately focusing on IoT product security or other individual parts of the ecosystem. ITI encourages stakeholders to take thoughtful, holistic approaches to managing both the security of devices and the networks and complex ecosystems that comprise global IoT security.

ITI appreciates METI's leadership in developing the Framework. We support METI's approach laid out in the Framework of taking a comprehensive, outcome-based approach to IoT security that focuses not only on products but also the networks and ecosystems. We encourage METI to consider our comments in the following areas:

- Consider referencing global best practices on IoT approaches
- Define key concepts using harmonized IoT definitions.
- Include technical measures that can improve IoT security at the connectivity/network level once a device or system is deployed.

General Comments

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

ITI supports METI's Holistic Approach to IoT Security that Focuses Beyond the Device
We agree with METI's assessment that focusing on device-level security (including utilizing certifications for such device-level security) by itself is not an effective policy approach to secure IoT. There are certainly security baselines that IoT device manufacturers should consider adopting, such as avoiding default passwords and keeping device software updated in a timely manner. However, focusing solely on IoT device security is an inefficient and oftentimes ineffective approach. Unfortunately, many policy proposals have narrowly focused on individual components of the ecosystem, rather than focusing on ecosystem security as a whole**.** For instance, some policies propose that internet service providers (ISPs) should simply shut down all botnets, or that manufacturers of billions of devices should make them universally secure. Such overly simplistic solutions fail to address the fundamental need to continuously secure the ecosystem. Regardless of which security measures are taken at the device, network, or software level, risks are ever present and ever evolving. Security does not start or end with any single component of the ecosystem.

The METI Framework also points out that focusing only on the security of a device does not account for several external variables such as environments and economic activities. Even the same device is not always used the same way, which results in differing risk profiles and potential impacts. Thus, we appreciate METI's approach in the Framework, which acknowledges the importance of considering the complex ecosystem in which IoT devices operate and encourages policymakers to take a comprehensive approach to IoT security, including at the network level. Given the fact that all IoT devices leverage networks to communicate, the network should be a priority detection and enforcement point for IoT security. We encourage METI to continue being a thought leader in IoT security by emphasizing the importance of networks and ecosystems to international partners.

Recommendations

Consider Referencing Global Best Practices on IoT Approaches
We recommend that METI consider referencing the following efforts in Section 3-3 Security and Safety requirements:

- 2nd draft of NIST 8259 IoT Device Manufacturers Foundational Activities and Core Baselines[1];
- C2 Consensus on IoT Device Security Baseline Capabilities[2]; and
- ISO/IEC 27402 IoT security and privacy – device baseline requirements (this is currently in progress).

In particular, NIST's ongoing work to develop IoT baselines has been integral to forging improved collaboration among industry, government, and academia on IoT security. ITI co-founded the Council to Secure the Digital Economy (CSDE) which published an International Anti-Botnet Guide[3] to identify practices and capabilities for combating botnets and other automated threats (a document which was cited multiple times in the Botnet Roadmap), and we participated in the

[1] NISTIR 8259 Recommendations for IoT Device Manufacturers Foundational Activities and Core Baselines, 2nd draft. https://csrc.nist.gov/publications/detail/nistir/8259/draft

[2] CSDE, The C2 Consensus on IoT Device Security Baseline Capabilities. https://securingdigitaleconomy.org/wp-content/uploads/2019/09/CSDE_IoT-C2-Consensus-Report_FINAL.pdf

[3] CSDE, International Anti-Botnet Guide. https://securingdigitaleconomy.org/wpcontent/uploads/2018/11/CSDE-Anti-Botnet-Report-final.pdf

CSDE-driven C2 consensus with approximately 20 other associations to develop a consensus industry position around IoT device security baselines. We recommend METI consider referencing those security baseline efforts in its Framework document and additionally follow the developments at ISO/IEC JTC1 SC27 in an effort to harmonize IoT approaches globally.

Define Key Concepts Using Harmonized Definitions on IoT

It would be helpful to synchronize definitions related to IoT security such as device, IoT device (line 60), and IoT device manufacturer (line 283). We recommend that METI leverage the following existing definitions:

- A ***device*** is a finished product which is usable for its intended functions without being embedded or integrated into any other product and is not a component.[4]
- An ***IoT device*** has at least one ***transducer*** (sensor or actuator) for interacting directly with the physical world, and at least one ***network interface***, and ***is not*** a conventional Information Technology (IT) device, such as smartphone and laptop, for which the identification and implementation of cybersecurity features is addressed under existing frameworks or a component. [5]
- An ***IoT device manufacturer*** is the entity that creates an assembled final IoT device.[6]

Components (which fail to meet the definitions of IoT device because they typically cannot function on their own in this context) are therefore beyond the scope of the IoT devices definition. Establishing clear definitions to separate IoT devices and ***general-purpose computing devices*** (such as personal computing system or smart phone) will allow the METI Framework to better address computing and security capabilities of the IoT devices in scope and ensure that the Framework is actionable and easy to apply.

Include Technical Measures to Secure IoT Networks

The perspectives offered in Section 3 of METI's Framework can help organizations to manage cybersecurity risks more effectively, including those presented by IoT. The organization of IoT security risks into three axes – the degree of difficulty of recovering from an incident, the economic impact of an incident, and the desired security and safety requirements are a helpful way to frame an organization's risk assessment. In particular, the third axis in Section 3-3 suggests that looking at desired IoT security and safety requirements during the manufacturing phase (Section 3-3-1) and during operation (Section 3-3-2) are both important. During the manufacturing phase, security requirements are a security indicator, which conveys that a product meets requirements at a certain point in time. However, METI's Framework (Section 3-1) also recognizes that even if security requirements are uniformly set, such requirements are not adequate to respond to all security challenges and users cannot always be protected. An IoT device might be built to the strongest security standards at the time of deployment, but at the end of the day problems can still occur,

[4] Compare to the definition of device manufacturer from ETSI TS 103645 Cybersecurity for Consumer IoT 3.1: Entity that creates an assembled final consumer IoT product, which is likely to contain the products and components of many other manufacturers; see also NISTIR 8259 line 288-289 ("The IoT devices in scope for this publication can function on their own and are not only able to function when acting as a component of another device, such as a processor"); see also ISO/IEC 27402 (in draft).

[5] This proposed definition includes defined terms: Transducer: A portion of an IoT device interacting directly with a physical entity of interest. The two types of transducers are sensors and actuator. Sensor: A portion of an IoT device providing an observation of an aspect of the physical world in the form of measurement data; Actuator: A portion of an IoT device changing something in the physical world.

[6] See also NISTIR 8259, Draft 2nd (referenced above).

including unforeseen technical challenges, human errors, or exploited vulnerabilities, or lack of good cyber hygiene. Thus, outcome-based operational security requirements are also essential.

We would also recommend that METI's Framework consider including technical recommendations at the network level, which can improve IoT security, including:

- Enable Constant Visibility of All Devices and Their Behaviors at All Times
  Organizations leveraging IoT devices and systems need to have constant real-time visibility and granular control across traffic passing through their networks. Only then can they detect and stop malicious threats and activities, such as IoT-based botnets. METI should encourage organizations to leverage technology to enable complete and continuous visibility of their networks and to enable discovery, identification, security, and optimization of their connected IoT devices.
- Adopt a Zero Trust Approach
  Under the Zero Trust concept, an organization should not automatically trust any unauthenticated activity inside or outside its network perimeters. Instead, an organization must authenticate every user or device trying to connect to its systems before granting access, including IoT devices. That level of granular control around key critical infrastructure and data allows cybersecurity risk management to become more effective.
- Segment Networks Where IoT Devices are Deployed
  Organizations that apply micro-segmentation of IoT devices based on device risk profiles are more likely to avoid cross-infections between IT and IoT systems. Through segregating and limiting the ability of legacy, low-patched and generally high-risk IoT devices to communicate with other IT assets, organizations can prevent threats from spreading across their networks.

ITI is pleased to respond to this public comment. We reiterate our industry's commitment to seek global harmonization and cooperation consistent with core baseline capabilities for IoT security, driven by industry consensus and grounded in global standards. We look forward to working with METI to ensure we can maximize the benefits of IoT while mitigating security risks and promoting best practices and solutions around IoT security globally.

Sincerely,

Naomi Wilson
Senior Director of Policy, Asia
Information Technology Industry Council