BSA Comments on the Draft of IoT Security Safety Framework

May29, 2020

BSA | The Software Alliance (**BSA**)[1] appreciates the opportunity to submit the following opinions to the Ministry of Economy, Trade and Industry (**METI**) on the Draft IoT Security Safety Framework (**draft Framework**).

General Comments

BSA's members are at the forefront of data-driven innovation, developing and offering essential software, security tools, communications devices, servers, and computers that drive the global information economy and improve our daily lives. Our members earn users' confidence by providing essential technologies, including industrial control systems and IoT solutions, that will form the backbone of the digitally connected industry envisioned in Society 5.0, and the security technologies to protect these users and technologies from cyber threats. Our members thus have significant interest in METI's draft Framework.

BSA provided comments[2] during the drafting of the Cyber/Physical Security Framework (**CPSF**). We appreciate the ongoing effort by METI to further advance the discussion, developing this draft Framework that focuses on the security of transcription and translation functions of devices and systems, including IoT, that connect cyberspace and physical space. We also commend METI for providing a sufficient period of time for industry consultation and for preparing English translations and accepting comments in English. BSA would like to offer the following specific comments to contribute to your efforts.

Specific Comments Regarding the Guidelines

International Interoperability

Ensuring interoperability at both the national and international levels are critical to driving effective security policies. Numerous governments including at the national level (Australia,[3]

[1] BSA's members include: Adobe, Amazon Web Services, Atlassian, Autodesk, AVEVA, Bentley Systems, Box, Cadence, Cisco, CNC/Mastercam, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Sitecore, Slack, Splunk, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

[2] https://www.bsa.org/files/policy-filings/02282019BSACommentsMETICPSFramework.pdf

[3] https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf

22F Shibuya Mark City West
1-12-1 Dogenzaka Shibuyaku,
Tokyo 150-0043

P +81 3 4360 5473
F +81 3 4360 5301
W bsa.org

Japan Representative Office

the European Union,[4] Japan,[5] Singapore,[6] and the United Kingdom[7]) and the state or provincial level (California[8] and Oregon[9] in the United States) have developed initiatives to address IoT security. As more governments rightly focus on this pressing issue, the risk of fragmentation among policies increases. National and international fragmentation in governments' IoT security policies is problematic because IoT solutions are inherently interconnected and interdependent. Fragmented policies can cause difficulties for enterprises offering products and services in many markets that may have divergent or contradictory requirements. Such outcomes can reduce competitiveness and stifle innovation, thus undermining the ability of end-users to access the most secure technologies.

As government approaches to IoT security take shape, multinational technology companies developing IoT solutions will face an increasingly complex landscape of policy guidance, regulatory requirements, and standards. Leading developers of IoT solutions offer their cutting-edge technologies worldwide, no matter where the underlying code was developed or the devices were manufactured. Such businesses will be harmed if national and international policies related to security and safety are disjointed, incoherent, or conflicting. Therefore, promoting internationally interoperable IoT security policies is a critical goal for the global economy.

Government IoT security policies should be informed by, and to the extent possible, aligned with other, similar efforts underway around the world.[10] To achieve this goal, government policies should be based on internationally recognized standards where available.

In this regard, BSA would like to bring attention some recent work in this area and recommend METI's review of the efforts listed below.

- The US National Institute for Standards and Technology (NIST) Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline (2nd Draft)[11]
- The C2 Consensus on IoT Device Security Baseline Capabilities (in revision)[12]
- ISO/IEC 27402 (in process) (IoT security and privacy – Device baseline requirements)

[4] https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot, https://www.enisa.europa.eu/publications/iot-security-standards-gap-analysis

[5] https://www.meti.go.jp/english/press/2016/0705_01.html

[6] https://www.imda.gov.sg/-/media/imda/files/regulation-licensing-and-consultations/consultations/open-for-public-comments/consultation-for-iot-cyber-security-guide/imda-iot-cyber-security-guide.pdf

[7] https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security

[8] https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327

[9] https://olis.leg.state.or.us/liz/2019R1/Downloads/MeasureDocument/HB2395/Enrolled

[10] E.g. ISO/IEC 19941:2017 is designed to increase interoperability between systems and is a reference for the European Interoperability Framework and other emerging frameworks for interoperability.

[11] https://csrc.nist.gov/publications/detail/nistir/8259/draft

[12] https://securingdigitaleconomy.org/wp-content/uploads/2019/09/CSDE_IoT-C2-Consensus-Report_FINAL.pdf

Consistent Definitions

BSA supports effective IoT security policies that include specific, understandable definitions aligned with international, consensus-driven, widely adopted standards for key terms, such as "IoT" and "IoT device". This is critical for clearly communicating policies' scope and intent to industry and other stakeholders, and to avoid inconsistent definitions.

In this respect, we recommend policymakers ensure IoT security policies define which devices are covered with the greatest specificity and clarity possible. In general, IoT security policies should use definitions for "IoT device" and "IoT systems" based on internationally recognized standards[13] that:

- refer to a device that is designed to connect to a network and includes computer processing capabilities necessary to collect, send, or receive data;
- refer to finished product available to end users that is usable for its intended functions without being embedded or integrated into any other product and is not a component;
- acknowledge that IoT devices are designed to be connected to a broader ecosystem that includes other components, devices, and systems; and
- do not include general computing devices, including personal computing systems, smart mobile communications devices, and mainframe computing systems.

Section 1-1-2: The positioning of the second layer, Lines 94-98

BSA recommends the example in this section emphasize the need for designers and implementers of IoT systems to consider additional physical security control measures based on the environmental condition where the IoT device will be installed, to protect critical IoT devices. The proposed use of physical separation as a required control is prescriptive and is not an effective or efficient approach when considering the dynamic and multi-faceted nature of the IoT environment highlighted in lines 55 to 57. Moreover, physical network separation may interfere with dynamic, effective, and efficient mechanisms for ensuring data integrity within acceptable parameters best implemented within the application that is collecting, processing, or handling data, because the accuracy of data collected by the IoT device at the physical layer and converted from analogue signals into the digital domain cannot be guaranteed.

Section 1-1-2: The positioning of the second layer, Lines 94-98
Section 3-2-1: Organization of hidden risks in devices and systems connecting physical space and Cyberspace

We also suggest considering additional approaches to risk management that complement the ***result/impact assessment*** process adopted in the proposed framework. The references of the recent efforts mentioned above (see Section on International Interoperability) contain helpful information about additional approaches to risk analysis in IoT.

Section 3-3-1 through 3-3-3: Confirmation Requirements

This section suggests the use of various confirmation requirements for security (voluntary attestation, certification, licensing, etc.). While many of these requirements would be beneficial for security, particularly in high-risk applications, international coordination should be leveraged in order to establish the criteria to ensure international interoperability of standards and elevate security protocols globally. We recommend METI further clarify the conditions for confirmation requirements.

[13] E.g. ISO/IEC 17788:2014 Information technology - Cloud computing - Overview and vocabulary; ISO/IEC 20924:2018 Information technology - Internet of Things (IoT) – Vocabulary; and ISO/IEC TR 23188:2020 Information technology - Cloud computing - Edge computing landscape

Conclusion

BSA hopes the above comments will be useful as you finalize IoT Security Safety Framework. BSA is currently developing principles on IoT security to support governments around the world in developing IoT security policies. We look forward to sharing these principles with METI once completed. We also remain happy to continue communicating with you in promoting greater security under new industrial environments. Please let us know if you have any questions or would like to discuss these comments in more detail.

22F Shibuya Mark City West
1-12-1 Dogenzaka Shibuyaku,
Tokyo 150-0043

P +81 3 4360 5473
F +81 3 4360 5301
W bsa.org

Japan Representative Office