The Cyber/Physical Security Framework (Draft)
Comments of BSA | The Software Alliance
May 28, 2018

BSA | The Software Alliance ("**BSA**")[1] welcomes this opportunity to provide our comments on the draft Cyber/Physical Security Framework ("**Framework**") issued by Ministry of Economy, Trade and Industry ("**METI**").

Statement of BSA Interest

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 security technologies to protect them from cyber threats. These threats may be posed by a broad range of malicious actors, including those who would steal our identities, harm our loved ones, steal commercially valuable secrets, or pose immediate danger to national security. Our members thus have a significant interest in METI's draft Framework.

BSA has worked closely with governments around the world in relation to the development of national cybersecurity policies and legislation. In doing so, we have witnessed first-hand the potential for such policies and legislation to effectively deter and manage cybersecurity threats whilst still protecting the privacy and civil liberties of citizens.

As a result of this experience, BSA has developed the International Cybersecurity Policy Framework ("**BSA International Framework**"), which sets out a recommended model for a comprehensive national cybersecurity policy. We have included a copy of the BSA International Framework with this letter.[2]

[1] BSA (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. BSA's members include: Adobe, Amazon Web Services, ANSYS, Apple, Autodesk, AVEVA, Bentley Systems, Box, CA Technologies, Cisco, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, Microsoft, Okta, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, The MathWorks, Trend Micro, Trimble Solutions Corporation, and Workday.

[2] The BSA International Framework is available on-line at https://bsacybersecurity.bsa.org/wp-content/uploads/2018/04/BSA_cybersecurity-policy.pdf. More information is available at https://bsacybersecurity.bsa.org/.

22F Shibuya Mark City West
1-12-1 Dogenzaka Shibuyaku,
Tokyo 150-0043
P +81 4360 5473
F +81 4360 5301
W bsa.org
Japan Representative Office

In summary, the BSA International Framework recommends six overarching principles that should guide the development of a successful national cybersecurity policy, namely that policies should:

1. be aligned with internationally recognized standards;
2. be risk-based, outcome-focused, and technology neutral;
3. rely on market-driven mechanisms where possible;
4. be flexible and encourage innovation;
5. be rooted in public-private collaboration; and
6. be oriented to protect privacy.

While these principles are framed to guide overarching national cybersecurity policies, we believe they are also highly relevant to the Framework and should inform its approach.

General Comments on the Draft Framework

BSA appreciates METI's efforts to encourage society as a whole to improve cyber and physical security and to educate all kinds of industries in Japan, including small- and medium-sized enterprises (SMEs) which play such an important role in supply chains, job-creation, and society. We understand such efforts will be a basis to realize Japan's vision for a reliable Society 5.0 and Connected Industries.

We are particularly grateful to METI for ensuring that the Framework addresses critical and emerging security topics, including the importance of supply chain security and discussing the concept of security by design and its increasing relevance for deployment of the Internet of Things ("**IoT**").

To improve the draft Framework, ***BSA urges METI to place greater emphasis on existing international standards and private-sector efforts*** around cybersecurity. The global supply chain consists of companies located in many different countries and internationally-standardized policies and practices are highly beneficial for allowing global businesses to provide, and benefit from, the best globally available security solutions. Companies in the private sector are voluntarily collaborating to share best practices and strengthen cybersecurity throughout their supply chains and customer bases; the Framework should embrace these efforts as means to strengthen cyber and physical security throughout industry and society.[3]

We applaud the Framework's citation of several internationally recognized technical standards during its discussion of specific security considerations. However, the Framework would benefit

[3] Good examples are Charter of Trust (https://www.siemens.com/innovation/en/home/pictures-of-the-future/digitalization-and-software/cybersecurity-charter-of-trust.html) and IoT Security Maturity Model (http://www.iiconsortium.org/pdf/SMM_Description_and_Intended_Use_2018-04-09.pdf)

22F Shibuya Mark City West
1-12-1 Dogenzaka Shibuyaku,
Tokyo 150-0043
P +81 4360 5473
F +81 4360 5301
W bsa.org
Japan Representative Office

from more clearly and strongly emphasizing the importance of aligning products, processes, and business practices with relevant internationally recognized standards conceptually throughout the document. Moreover, we note the draft Framework references internationally recognized standards for *information security management systems (ISMS)* (ISO/IEC 27001), *cyber security management systems (CSMS)* (ISO/IEC 62443-2-1), *embedded device security assurance (EDSA)* (ISO/IEC 62443-4-2), and *information technology service management systems (ITSMS)* (ISO/IEC 2000) as examples of measures at certain places. However, the draft Framework omits mentioning other important internationally recognized standards such as ISO/IEC 27103, which is the recently published ISO/IEC technical report on critical infrastructure cybersecurity that aligns with the *Framework for Enhancing Critical Infrastructure Cybersecurity* developed by the US National Institute for Standards and Technology, and ISO/IEC 27034 (concerning the secure development lifecycle).

It is important to ensure that the Framework is not interpreted as advocating for the development and implementation of local requirements for cybersecurity which may be inconsistent with internationally recognized standards and best practices. Not only would this result in additional compliance costs to companies doing, or seeking to do, business in Japan, but such an interpretation risks diminishing Japan's leadership in promoting seamless, interoperable standards regimes globally.

We also observe that the recommended measures in the Framework appear targeted at different audiences — at consumers (purchasers of products) as well as suppliers (including producers or manufacturers of products). As such, there is ambiguity in terms of which recommended measures are applicable in a given scenario. For example, L1.008 and L1.009 would be more applicable to consumers, as they refer to a user organization needing to put in place a structure for detecting incidents and business continuity plans, respectively. However, L2.006 would be more applicable to suppliers, as it refers to the prevention of unauthorized logins through access control, something which is typically implemented by the supplier, and which a consumer would not be in a position to verify has been done by the supplier. L2.011 is another example of a recommendation that would be more applicable to suppliers — the countermeasures against counterfeit software would need to be built or implemented by the supplier and not a consumer.

The requirements also do not factor in the possibility that different IoT devices have different capabilities and not all IoT devices are able to implement the range of features and capability envisioned by the requirements. In relation to this, the various product features proposed by the Framework (e.g., identification of counterfeit software in L2.011, vulnerability countermeasures in L2.013, and having different functions accessible by different users) depend on how much computing power there is in the device to implement them; a 'dumb' IoT device would not be able to handle these requirements.

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

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

Japan Representative Office

Given the rapid advancement of technology, and the corresponding evolution of the cyber threat environment, **we applaud METI for developing a robust, voluntary Framework informed by internationally recognized technical standards and best practices, and we look forward to working with METI to further strengthen the Framework and urge its widespread use and continuing evolution.** While we believe it would be counterproductive for the Framework to be applied as a rigid prescriptive measure, it has great value as a set of best practices. The recommendations we provide herein are intended to strengthen its impact and facilitate its broad adoption.

Specific Comments on Draft Framework

In addition to the general comments above, BSA would like to offer the following comments and recommendations on specific portions of the draft Framework:

1. The First Layer

BSA recommends that the Framework address the following considerations in the first layer:

- Traceability: As a supply chain risk management best practice, companies should ensure they can trace all component parts to their original source.
- Data security: All supply chain data and sensitive product data should be protected at rest and in transit using encryption or other security tools.

2. The Second Layer

L2.002 Implementation of security by design into IoT devices:

- BSA applauds METI for including "security-by-design" into the draft Framework. Building software according to security-by-design principles generates safer, less vulnerable, better functioning software, and encouraging adoption of secure-by-design software can help drive adherence to such principles throughout the software sector. The section could be further enhanced with a more robust description of what "security-by-design" means.[4] To that end, the section should cite ISO/IEC 27034 (Application Security), which provides guidance to assist organizations in integrating security into the processes used for developing and managing software applications.

[4] Among other sources, core security-by-design principles are articulated in SAFECode's "Fundamental Practices of Security Software Development, Third Edition" (available on-line at: https://safecode.org/publications/#safecodepublications-2362) and the Open Web Application Security Project (OWASP; available online at: https://www.owasp.org/index.php/Security_by_Design_Principles).

22F Shibuya Mark City West
1-12-1 Dogenzaka Shibuyaku,
Tokyo 150-0043
P +81 4360 5473
F +81 4360 5301
W bsa.org
Japan Representative Office

L2.010 Appropriate disposal of IoT devices:

- BSA recommends this section not only discuss how to dispose of IoT devices, but also include guidance for proactively replacing IoT devices as necessary to maintain currency or when they are no longer supported by the manufacturer.

L2.013 Continuous vulnerability countermeasures for IoT devices:

- BSA recommends specifying that organizations should consider "patchability" in IoT device acquisition decisions as devices should be patchable absent exceptional circumstances. The guidance should also recommend "immediate" or "as quickly as possible, rather than "periodic," application of patches since security patches should be applied as quickly as possible upon release, with priority given to those patches addressing high-risk vulnerabilities.

3. The Third Layer

L3.014 Separation of networks:

- BSA urges METI not to promote physical separation of networks in general, since physical separation will jeopardize Japan's vision of "Society 5.0" and "Connected Industries" and often will not enhance security. Physically separated networks should be reserved to specific cases of highly sensitive data where, in addition to physical separation, other important features to mitigate the security risks introduced by physical separation are included.

4. References

As mentioned in our general comments above, there are other important international standards that the Framework should draw upon and refer to. We therefore recommend listing other important ISO/IEC standards such as ISO/IEC 27103, which provides guidance on how to leverage existing standards in applying a cybersecurity risk management framework, and ISO/IEC 27034, described above, in this section of the Framework. It would also be helpful to reference the NIST Interagency Report 7622 on supply chain risk management.

Conclusion

BSA and our members hope our comments will be useful as you finalize the draft Framework, and we welcome the opportunity to work with METI on refining the draft Framework. Please let us know if you have any questions or would like to discuss these comments in more detail.

-End-

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

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

Japan Representative Office