The Cyber/Physical Security Framework (Draft)
January 2019 Version

BSA | The Software Alliance Comments
February 28, 2019

BSA | The Software Alliance (**BSA**)[1] welcomes this opportunity to provide our comments on the updated draft Cyber/Physical Security Framework (**Framework**) issued by Ministry of Economy, Trade and Industry (METI) for public consultation on January 9, 2019.

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 technologies, including industrial control systems and Internet of Things (IoT) devices, 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. 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.

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 grateful for METI's leadership in seeking to address security challenges facing industrial supply chains, which are daunting and an increasing focus of policy-makers around the world.

BSA was grateful for the opportunity to provide comments on the initial draft of the Cyber/Physical Security Framework in 2018. The updated draft Framework in 2019 represents a substantial improvement, and we were grateful to see many of our earlier comments taken into consideration. In general, the updated draft provides an important tool to help industry stakeholders assess, manage, and respond to risks across the systems and networks they manage and the supply chains they maintain. We welcome a risk management approach that METI has taken in the framework that would be more effective than a prescriptive regulation approach. It is all the more powerful thanks to its conscious alignment with existing internationally recognized best practices, such as key ISO standards. In our previous comments, we urged METI to align the Cyber/Physical Security Framework with the *Framework for Enhancing Critical*

[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, Akamai, Amazon Web Services, Apple, Autodesk, AVEVA, Bentley Systems, Box, Cadence, Cisco, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, Siemens PLM Software, Slack, Splunk, Symantec, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

Infrastructure Cybersecurity,[2] and we are grateful for the updated draft's substantial attention to harmonizing these frameworks. This alignment enables technology developers to adapt approaches to security across international markets, collaborate to address emerging security threats across national boundaries, and build a global workforce trained around common concepts.

We continue to caution against adopting a Japan-specific framework to Cyber/Physical Security. We recognize that METI is developing guidance that in some ways goes beyond the current internationally-recognized frameworks by focusing on the integration of IoT with cloud computing. Existing frameworks, such as ISO's work on ISO/IEC 30141:2018 and ISO/IEC 17789:2014 which establish a reference architecture to map the applicability of existing ISO standards to IoT and cloud computing, leave significant gaps in implementation guidance. As such, as the Government of Japan pursues the development and application of the Framework, we urge METI to continually revisit the document to ensure maximum alignment with emerging internationally-recognized standards to avoid inadvertently creating confusion in the industry and undermining the benefits of interoperability with other efforts (e.g. in the United States, the European Union, and elsewhere) to promote IoT security.

In addition to the general comments above, BSA would like to offer the following specific comments on several elements of the current draft Framework.

Parts I and II: Three Layers and Six Elements

The model articulated by the draft Framework, identifying three layers ("connections between organizations," "mutual connections between cyberspace and physical space," and "connections in cyberspace") and six elements (people, organizations, systems, components, data, and procedures) provides a useful concept for understanding key actors and relationships in the digital industrial ecosystem. It usefully illustrates where responsibilities and security considerations may overlap, and where they may diverge. Moreover, it prompts cybersecurity personnel to consider resources or relationships in relation to security planning that may not be obvious in the complex ecosystem of modern digital industrial supply chains.

The three layers of the model translate usefully into an analytical tool to guide risk management activities, as Appendix A of the draft demonstrates.

On the other hand, the six elements will be most useful as an illustrative concept rather than as an analytical tool. We are concerned that, as an analytical tool, the six elements may introduce too much complexity and ambiguity for straightforward application by many cybersecurity professionals. It may be worth considering whether, in Part II particularly, the model can be simplified to help cybersecurity professionals target their limited resources in developing organizational cybersecurity plans and policies.

Part III: Security Measures

The Framework is well aligned with internationally recognized best practices and provides broad coverage of considerations critical to securing digital industrial ecosystems and supply chains. We offer specific comments regarding potential improvements to the security measures for your consideration in the table below.

CPS Reference	Draft Language	Comment
CPS-AM	Asset Management (General Comment)	The current draft section on Asset Management importantly includes guidance to maintain inventories of all hardware and

[2] https://csrc.nist.gov/publications/detail/white-paper/2018/04/16/cybersecurity-framework-v11/final

		software and to create records of information such as production date and condition. It should also include guidance that organizations adopt transparent and verifiable software asset management (SAM) practices to ensure that software is not only inventoried, but also confirmed to be appropriately licensed and up to date. Because unlicensed software is less likely to receive critical security updates that would otherwise mitigate the risks associated with malware exposure, its use heightens the risk of harmful cybersecurity incidents. Unlicensed technology from untrusted sources may also contain embedded malware inserted by malicious actors. **We recommend including, after the current CPS.AM-4, a new ID statement:** "**CPS.AM-X. Apply transparent and verifiable software asset management practices to ensure software is appropriately licensed and up to date.".** The relevant internationally recognized standard is ISO 19770-1.
CPS.AM-5	"Create and store a list of external information systems where the organization's assets are shared."	The "Guidebook for using Cloud Security Guideline" (METI, 2013) is a useful reference regarding points to consider when stipulating contractual terms regarding the roles and responsibilities of users, especially in terms of using cloud services. The following internationally-recognized standards also useful for this purpose: • ISO/IEC 17789:2014, Information technology — Cloud computing — Reference architecture • ISO/IEC 19086-1: 2016, ISO/IEC 19086-1:2016, Information technology — Cloud computing — Service level agreement (SLA) framework — Part 1: Overview and concepts • ISO/IEC 19086-4: 2019, ISO/IEC 19086-4:2019, Cloud computing — Service level agreement (SLA) framework — Part 4: Components of security and of protection of PII
CPS.AM-6	"Classify and prioritize resources (e.g., people, goods,	While classifying assets according to function, importance, and business value is important to effective asset management, it may make less

	data, and systems) by function, importance, and business value, and communicate to relevant parties.”	sense to classify people accordingly. Individuals within an organization can present similar security challenges (e.g., poor cyber hygiene, insider attack) regardless of their comparative importance of business value. **We recommend your strike “people,” from the ID statement.**
CPS.BE-3	“Identify the dependency between the organization and other relevant parties and important functions of each in the course of running the operation.”	This statement appears somewhat redundant of CPS.AM-2. **We recommend that you delete CPS.AM-2.**
CPS.GV	Governance (General Comment)	An essential practice for achieving strong cybersecurity governance is to ensure that cybersecurity information is communicated to an organization’s senior leadership, including its corporate officers and its Board of Directors, where relevant. **We recommend you add, following CPS.GV-4, a new ID statement:** **“Establish a process for communicating key information on cybersecurity risk management policies and significant cybersecurity incidents to the organization’s senior leadership.”**
CPS.RA-1	“Identify and document the vulnerability of the organization’s assets.”	It is unclear whether this ID statement calls for a simple assessment and documentation of the aggregate vulnerability and an organization’s assets, or if it would call for an assessment and documentation of the individual vulnerabilities. It is important that the recommendation is for the latter, that organizations should identify and document the individual vulnerabilities of their assets.
CPS.SC-2	- Identify, prioritize, and evaluate the relevant parties crucial to sustaining the operation of the organization.	For the purposes of clarity and ease of use, the ID statement should be broken out into several separate statements. Moreover, the draft statement currently provides guidance to use IoT devices certified by a third party or self-attested to be safe and secure; however, it does not link to any sort of standard or

	- When devices are procured, select suppliers of IoT devices whose management systems are properly established and operated and whose help desks and support systems are well prepared. - Introduce the IoT devices certified by a third party or IoT devices confirmed by self-attestation for safe and secure use. - In services and system operations, select service suppliers who efficiently and effectively operate and manage services.”	benchmark against which IoT devices should be assessed. Absent such a standard or benchmark, certifications or self-attestations may communicate wildly divergent information about the safety and security of an IoT device. **We recommend that the draft language on use of certified IoT devices be deferred until future iterations (e.g. when more widely vetted IoT security standards exist), and that the ID statement be reorganized as follows:** **“CPS.SC-2. Identify, prioritize, and evaluate the relevant parties crucial to sustaining the operation of the organization.** **“CPS.SC-X. In services and system operations, select service suppliers who efficiently and effectively operate and manage services.** **“CPS.SC-X. When devices are procured, select suppliers of IoT devices whose management systems are properly established and operated and whose help desks and support systems are well prepared.”**
CPS.AC-6	Adopt multi-factor authentication, combining more than two types of authentication when logging in to the system over the network for the privileged user.”	We strongly support the use of multi-factor authentication to protect access to networks and other sensitive assets. Recent technological developments have enabled additional risk-based approaches to authentication (such as the use of contextual information like geolocation, device recognition, and pattern analysis), which can often be used in tandem with multi-factor or biometric identification. **Therefore, we recommend the ID statement be edited as follows:** “Adopt multi-factor authentication, combining more than two types of authentication **and/or other risk-based authentication techniques,** when logging in to the system over the network for the privileged user.”
CPS.DS-6	“Carry out periodic quality checks, prepare standby	Maintaining software with version upgrades and security patches is critical to both network and IoT security. **As such, we recommend**

	devices and uninterruptible power supplies, provide redundancy, detect failures, conduct replacement work, and update software for IoT devices, communication devices, circuits, etc.”	**devoting a distinct ID statement to this important security measure, as follows:** “CPS.DS-6: Carry out periodic quality checks, prepare standby devices and uninterruptible power supplies, provide redundancy, detect failures, **and** conduct replacement work~~, and update software~~ for IoT devices, communication devices, circuits, etc. “**CPS.DS-X: Ensure software assets, including IoT devices, are maintained with all current upgrades and security patches.”**

It may be useful for the Framework to refer to the definitions and usage of the following terms found in the relevant ISO international standards.

（1） “Actuator” to [SOURCE: ISO/IEC 20924:2018, 3.2.2]
（23） “Hash value” to [SOURCE: ISO/IEC 27037:2012, 3.11]
（24） “Identifier” to [SOURCE: ISO/IEC 20924:2018, 3.1.21]
（28） “IoT(Internet of Things)” to [SOURCE: ISO/IEC 20924:2018, 3.2.1]
（29） “IoT device” to [SOURCE: ISO/IEC 20924:2018, 3.2.4]
（56） “Sensor” to [SOURCE: ISO/IEC 20924:2018, 3.2.9]
（57） “Service” to [SOURCE: ISO/IEC TR 17028:2017, 3.1]
（64） “Timestamp” to [SOURCE: ISO/IEC 18014-1:2008, 3.12]
（65） “Trustworthiness” to [SOURCE: ISO/IEC 20924:2018, 3.1.32]
Also, check “IoT Trustworthiness” to [SOURCE: ISO/IEC 20924:2018, 3.2.10]

Conclusion

Once again, we applaud METI for developing a robust, voluntary Framework informed by internationally recognized technical standards and best practices, and we are grateful for METI’s efforts to address many of our previous comments in its updated draft. BSA and our members hope our comments will be useful as you continue development of the draft Framework, and we welcome the opportunity to work with METI as the effort proceeds. Please let us know if you have any questions or would like to discuss these comments in more detail.