Comments from BSA | The Software Alliance on Draft Basic Guidelines for Ensuring the Stable Provision of Specified Social Infrastructure Services Through the Prevention of Specified Interference Actions

March 10, 2023

General Comments

BSA | The Software Alliance (**BSA**)[1] welcomes the opportunity to provide comments to Economic Security Promotion Office on the draft "Basic Guidelines for Ensuring the Stable Provision of Specified Social Infrastructure Services Through the Prevention Specified Interference Actions" (**Basic Guidelines**).

BSA is the leading advocate for the global enterprise software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, providing cutting-edge technologies and services that power governments and businesses including cloud computing, data analytics, and artificial intelligence (**AI**). BSA members are also leaders in security, having pioneered many of the software security best practices used throughout the industry today.[2]

BSA works closely with governments around the world on developing cybersecurity policies. Based on these experiences, we provide our comments below to support the efforts of the Government of Japan (**GOJ**). As BSA shared in the earlier submission[3], as a general matter, we recommend GOJ to design sustainable and transparent approach to effectively identify and disrupt malicious acts. The Basic Guidelines presents the current considered direction to implement the new pre-examination scheme stipulated in Chapter 3 of "Act on Promotion of

[1] BSA's members include: Adobe, Alteryx, Altium, Amazon Web Services, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, Dassault, Databricks, DocuSign, Dropbox, Graphisoft, IBM, Informatica, Juniper Networks, Kyndryl, MathWorks, Microsoft, Nikon, Okta, Oracle, Prokon, PTC, Rockwell, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

[2] See *Strengthening Trust, Safeguarding Digital Transformation: BSA's Cybersecurity Agenda at* https://www.bsa.org/files/policy-filings/10132021bsacybersecurityagenda.pdf and *The BSA Framework for Secure Software: A New Approach to Security the Software Lifecyle – Version 1.1 (September 2020)* at https://www.bsa.org/files/reports/bsa_framework_secure_software_update_2020.pdf

[3] https://www.bsa.org/policy-filings/japan-bsa-recommendations-on-promoting-japans-economic-security

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

Ensuring Security by Taking Economic Measures in an Integrated Manner" (**Act**), including designating specified social infrastructure business operators, critical facilities, and entrustment for the maintenance/management of critical facilities. As the Basic Guidelines rightfully acknowledge, it is important to minimize unintended consequences that may interfere with the technologies and economic activities the new system is designed to protect and ensure these policies to not impede innovation and access to the best available technology globally. BSA looks forward to collaborating with the GOJ to enhance the security, integrity, and vitality of Japan's digital economy.

Chapter 3 Matters to be Considered in Ensuring Stable Provision of Specified Social Infrastructure Services by Preventing Specified Interference Actions

Section 1 Basic Consideration on Specified Critical Facilities / (1) Basic Consideration on Specified Critical Facilities

Section 1 (1) of Chapter 3 of the Basic Guidelines highlight facilities, equipment, devices or programs that are important for the stable provision of Specified Social Infrastructure Services. One of the causes of disruption or causes of deterioration is not due to acts of interference, but the use of equipment, systems or software that are no longer supported by the vendor or supplier of the equipment, system or software. For instance, physical networking products used by telecom operators that reach their end-of-life should no longer be used and should be replaced with updated products that are supported. Similarly, software products that are no longer supported should be replaced with updated versions.

We recommend that for specified critical facilities, a prohibition be instituted on the continued use of end-of-life equipment, system and software that are no longer supported by the product vendor. This will help to minimize disruptions arising from such outdated products. End-of-life notifications of products are usually given well in advance of the date of the end of support. Operators of specified critical facilities should plan for migration and upgrade upon such notification of end-of-life of products.

(2) Consideration on Change of Programs

Section 1 (2) of Chapter 3 of the Basic Guidelines present the policy regarding specified critical facilities, equipment and devices that include programs. It stipulates that when changes are made to the functions related to the programs listed in submitted installation plan (including new additional functions), in principle, these changes must be notified or reported to the Government. While the official designation of specified critical facilities remains to be determined, should cloud computing be included in the scope, it will be helpful for cloud service

providers (**CSPs**) and their customers to have clear and practical guidance to effectively implement such policy. This includes defining what kind of cloud services will fall as “installation” or “entrustment” of Specified Critical Facilities by Specified Social Infrastructure Business Operators under the Act. It is particularly important that the definition of such cloud services stipulated by various competent ministries remain consistent. To avoid fragmentation including such definition, we strongly urge the Cabinet Office and Cabinet Secretariat to take strong leadership in providing high-level guidance which will be adopted across ministries, including creating safety standards for systems which are commonly used in many industries. Such guidance will also be helpful in identifying areas of harmonization and also decisions that will be left to individual ministries.

We also recommend, upon developing policies and ministerial ordinance, to take into consideration the cloud-specific aspects to appropriately guide private sector as well as to enable Specified Social Infrastructure Business Operators to smoothly transition to cloud under the Act. For example, the Basic Guidelines clarify that minor changes, such as daily updates that fix bugs, are not required to be notified. Given the constantly evolving nature of cloud services, it is also important to understand that regular updates are conducted globally and simultaneously by CSPs. These changes are necessary to quickly respond and improve services, including security, for customers. If updates of functions are also subject to the notification obligation as “change of programs”, it will create confusion in actual business operation. Therefore, the Basic Guidelines can further be improved by clarifying that notification, etc. is limited only to those changes that have a substantial impact on risk management, to appropriately guides cloud users in designated businesses.

Section 3 Matters to be Considered in Formulating the Ordinance of the Competent Ministry Designating Specified Critical Facilities and Critical Maintenance/Management, etc.

The “Basic Policy on Promotion of Ensuring Security by Taking Economic Measures in an Integrated Manner” (decided by the Cabinet on September 30, 2022), presented basic matters to take into consideration upon implementing the Act, including maintaining compatibility with free and fair economic activity. In line with this Basic Policy, Section 3 of Chapter 3 in the Basic Guidelines further elaborates that the ordinance from competent ministers designating specified critical facilities and critical maintenance/management, shall carefully consider determination so as to not unreasonably impede proper competitive relationships and to limit the scope to what is truly necessary, to avoid excessive burdens in the provision of Specified Social Infrastructure Services. BSA recommends the GOJ take into account the global security practices and internationally recognized standards to assess the level of security and to present clear guidance to CSPs and their customers to enable cloud-based systems to be installed smoothly while complying with the Act and ministerial ordinance.

Further, with regards to the burden to be placed on suppliers, in light that new cyber threats and vulnerabilities will continually emerge, and it would be important that updates and measures provided by vendors are applied in a timely manner, we would encourage flexibility in the approach taken to apply the measures to allow threats to be effectively addressed.

Chapter 4 Basic Matters Regarding Recommendations and Orders to Specified Social Infrastructure Business Operators

Section 1: Consideration on Notification of Installation Plan and Recommendation and Order

(4) Factors to be Considered in the Examination

Chapter 4, Section 1 (4) presents factors to be considered in assessing risks during the pre-examination process, stating that “it is necessary to carefully examine the installation of facilities from business operators that are strongly influenced by entities outside of Japan”. While we understand that influence from foreign governments will be concerning factors under the examination, it would be helpful for involved stakeholders to understand whether the factors to be taken into consideration extend to suppliers that have relations with overseas entities influencing local entity, such as relationship between the headquarters and subsidiary or affiliated companies in Japan.

With regard to the examination of influence by entities outside of Japan, clarification regarding the scope and limits of the responsibility of the different stakeholders who can be potentially involved in such a situation will be useful to avoid imposing unnecessarily burdensome obligations on a single stakeholder.

(5) Risk Management Measures

Section 1, (5) of Chapter 4 lists examples of risk management measures that Specified Social Infrastructure Business Operators can take to mitigate the risks upon installing Specified Critical Facilities and entrusting Critical Management/Maintenance and indicates that implementations of the measures are factors necessary to examine the risks of specified critical facilities being used as a means of specified interference actions. While there are industry specific systems etc., it is important to note that there are also commonly used systems in many industries including telecommunication, etc. For such commonly used systems, we strongly recommend setting common regulatory requirements including how to manage and examine risks and the type of information required to

be submitted. We further recommend that these requirements be based on internationally recognized standards whenever possible.

The Government should also take into account the potential of cloud services enhancing data protection and improving cybersecurity through cost-effective approach, such as confidential computing and zero-trust principles. We also encourage the risk evaluation criteria incorporate existing international benchmarks, best practices, and certification frameworks. For cloud service, these may include recognizing ISO/IEC 27001, 27017 and 27018, Information system Security Management and Assessment Program (**ISMAP**), other relevant standards and third-party certifications. Further, we also recommend recognizing authorization from like-minded countries, such as US Government's Federal Risk and Authorization Management Program (**FedRamp**) as having appropriate cybersecurity risk management processes in place. In order to enable effective implementation of the system, it is important to avoid creating duplicative regulations that would result in excessive burden on Specified Social Infrastructure Business Operators and their suppliers. The integration of internationally recognized standards and other programs in risk evaluation will facilitate efficient and effective implementation of pre-examination and will provide greater clarity and certainty for the diverse business operators that may be covered under this new system.

The aim of the risk evaluation criteria should be to guide business operators as they seek to establish risk thresholds and understand their risk tolerance. The Basic Guidelines should provide that examination of risks should also include the assessment of the level of risk posed by specified critical facilities, laying down the responsibilities of the business operators to apply requisite mitigation measures according to the level of risk posed. If the obligations are imposed based on the risk-level, business operators will not need to spend excessive resources on managing immaterial or low-level risks. Illustrative examples can be included in this regard, clarifying that they are merely examples and not a categorical determination.

Chapter 5 Matters Concerning Cooperation with Specified Social Infrastructure Business Operators and Other Relevant Stakeholders Necessary to Ensure Stable Provision of Specified Social Infrastructure Services by Preventing Specified Interference Actions

Section 3 Appropriate Consideration of Opinions of Stakeholders, etc.

Chapter 5, Section 3 indicates that "in formulating cabinet ordinance and ministerial ordinances, the Prime Minister and competent ministers shall fully listen to the opinions of industry associations, academic experts, relevant administrative

agencies, and other persons with knowledge and experience from ordinary times. In addition, the public comment system shall be utilized, and diverse opinions shall be appropriately considered". While we welcome such strong commitment to listen to the opinions of stakeholders, we also note that the period for this public comment process allows just one month to respond, which does not provide sufficient time for stakeholders to fully comprehend and consider substantial comment. Given that foreign business operators require considerable time to prepare English translation, we urge the Government to ensure at least two months for the public comment period, as well as provide English version of the draft upon launching public consultation.

Conclusion

BSA looks forward to working with the GOJ to support its goal of effectively promoting economic security. In addition to submitting the comments, we would appreciate having continued opportunities for dialogue to better understand the considered directions, in order to provide further recommendations and suggestions to assist the GOJ in achieving its objectives.