Recommendations from BSA | The Software Alliance on Promoting Japan's Economic Security

April 26, 2022

General Comments

BSA | The Software Alliance (**BSA**)[1] supports efforts by the Government of Japan (**GOJ**) to strengthen the stability of specific social infrastructure services and managing associated security risks, reducing Japan's vulnerability to acts of sabotage or other acts of aggression that could put specific social infrastructure services at risk.

As GOJ considers enacting the *Act on the Promotion of Ensuring Security Through the Integrated Implementation of Economic Measures* and works to develop basic policies to implement a new pre-examination system, including designating specific services, business operators, critical equipment, and services consigned for the maintenance/management of critical equipment, 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 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 the observations and recommendations below to support the GOJ's efforts. As a general matter, we recommend GOJ to adopt effective approaches to risk management that recognize the global, interconnected nature of today's technologies and the threats against them, to design sustainable and transparent policy

[1] BSA's members include: Adobe, Alteryx, Altium, Amazon Web Services, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, Dassault, DocuSign, Dropbox, IBM, Informatica, Intel, MathWorks, Microsoft, Nikon, Okta, Oracle, PTC, Rockwell, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, 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

responses to effectively identify and disrupt malicious acts. We look forward to collaborating with the GOJ to enhance the security, integrity, and vitality of Japan's digital economy.

Ensure transparent processes involving robust public consultation, and frequent review.

Understanding how policies will be effective against the threat they are intended to mitigate will necessitate open and candid dialogue with affected stakeholders, including industry. We strongly recommend GOJ to make the process of developing these policies and their implementation transparent, engaging with private sector through meetings and public consultations. As industry increasingly provides leadership on responding to security concerns, we recommend GOJ to embrace creative opportunities for public-private partnerships aimed at ensuring economic security and developing best practices for risk management through regular review after implementation.

Ensure policies are narrowly tailored.

To effectively achieve their goals, polices should be targeted to address specific objectives in a manner that is minimally disruptive to Japan's interests, avoiding overly broad scoping that makes implementation impractical and ineffective. As competent ministries consider the designation of specific social infrastructure services, operators, equipment, and services consigned for the maintenance/management of those equipment, we strongly recommend limiting the scope of covered entities, equipment, and services to those that are most essential to enable business operators to deploy their products and services with minimal delay and to avoid undermining innovation.

Ensure policies are cohesive and holistic.

We also strongly encourage ensuring that policies remain consistent and coordinated across government agencies. As competent ministries work to set requirements to evaluate and determine security risks for the proposed pre-examination system, policy makers should consider whether specific decisions are consistent with the overall strategic objective, including by identifying unintended consequences that may result from any specific action. It is also important that unified requirements and formats for prior notification are adopted across agencies to provide clarity for all stakeholders involved, including the business operators that provide specified equipment and services to designated social infrastructure services.

Ensure policies embrace clear and well-defined criteria.

Modern technologies are often transnational, and so too are threats against them. As such, effective policies should avoid adopting categorical prohibitions against the acquisition or installment of technologies simply because they are developed abroad. We encourage the risk evaluation criteria to be clear and well-defined and incorporate international benchmarks, best practices, and certification frameworks. For cloud service, these may include recognizing ISO/IEC 27001, 27017 and 27018, and other relevant standards and third-party certifications. 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. Clear and well-defined criteria based on internationally recognized standards will also enable GOJ to access the most innovative products and competitive prices.

Ensure policies are risk-based.

We recommend GOJ to adopt risk management approaches that retain sufficient flexibility to enable security practitioners within both government entities and businesses to adapt to a constantly evolving threat environment. To avoid unintended consequences of mistargeted policies, it is important that risk management approaches consider not only risks from malicious actors, but also the risks, timelines, and costs associated with proposed mitigation measures, and most importantly, recognize that malicious actors will constantly improve their tactics, techniques, and procedures.

Conclusion

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