BSA Comments on
ICT Cybersecurity Comprehensive Measures 2021 (Draft)

July 8, 2021

BSA | The Software Alliance (**BSA**)[1] appreciates the opportunity to submit the following comments to the Ministry of Internal Affairs and Communications (**MIC)** on the "ICT Cybersecurity Comprehensive Measures 2021 (Draft)" (**draft Measures)**.

General Comments

BSA is the leading advocate for the global software industry in the international marketplace. Our members are at the forefront of software-enabled innovation that is fueling global economic growth, including cloud computing, the Internet of Things (IoT), artificial intelligence (AI), and other products and services that bring new innovation. BSA members are also leaders in security, having pioneered many of the software security best practices used throughout the industry today.

BSA filed comments[2] last year on the draft IoT/5G Security Comprehensive Measures 2020 and appreciates MIC's ongoing efforts to improve cybersecurity, with enhanced focus to promote Japan's digital transformation and creating an environment for safe utilization of various digital services by citizens. We also support MIC's efforts to develop high level guidelines for organizations to adopt and use technologies in IoT, 5G and cloud-based services in safe and secure ways, and appreciates acknowledging the importance of telework and to utilize cloud-based technologies in close coordination with international cybersecurity communities.

To support MIC's goal to ensure cybersecurity of ICT infrastructure and services to realize "free, fair and safe cyberspace", we provide the below observations and recommendations.

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

[2] https://www.bsa.org/files/policy-filings/062520japan_commiot5gsec_0.pdf

Observations and Recommendations

II. Specific Measures for Individual Sector of Information and Communication Services and Networks / 3 (2) Responses Based on the Progress of Use of Cloud Services

Whilst there have been outages and setting errors by end users as mentioned in draft Measures, these do not differ in a material way to on-premise and other similar alternatives, and the security tools available in the cloud today, together with the shared responsibility model, are comprehensive to ensure the highest levels of security practices.

As the draft Measures rightfully acknowledges, cloud computing can bring enormous benefits including cost reduction, rapid improvement of information systems, flexible increase and decrease of resources, and high reliability through automated operations, countermeasures for disasters, and realization of a telework environment. Cloud computing also offers substantial benefits to cybersecurity. In order for Japan to realize digital transformation and to fully leverage these benefits, the widespread adoption of cloud computing services by governments will be critical, and for this purpose, as indicated in the draft Measures, “Information system Security Management and Assessment Program” (ISMAP) was launched last year to assess the security of cloud services procured by government agencies. While we are encouraged with the establishment of this new mechanism that sets baseline security requirements for cloud service providers (CSPs), we are also concerned that the implementation of the ISMAP has become too cumbersome and costly to facilitate the Government of Japan’s goal of achieving “cloud-by default” in the public sector and to support Japan’s cybersecurity efforts to enable full-scale digital transformation.

With over 1,000 listed controls in ISMAP, there is significant compliance burden and prohibitive costs imposed on companies offering services and wishing to achieve ISMAP certification, and this reduces the attractiveness of ISMAP certification for many CSPs. This could result in unnecessarily limiting the number of CSPs registered in ISMAP Cloud Service List and eligible to provide their services to Japanese public sector entities.

As such, we recommend the Government of Japan continue to improve the ISMAP, including by:

- Making the ISMAP more flexible and implementable by better taking into account the distinctive requirements of different types of cloud services (SaaS, IaaS, PaaS) and defining essential security controls tailored to manage the risk to these respective services.

- Limiting the application of ISMAP to a set of core, fundamental security controls, and leaving additional security controls to be applied as needed given the specific context in which they are deployed and based on widely adopted internationally recognized cloud security standards, and any additional requirements in the commercial agreements established with procuring entities.

• Establishing a less frequent auditing schedule in line with international cloud security best practice (e.g., once every three years) to reduce the audit overheads for CSPs and the Government of Japan alike. Yearly audits could result in CSPs conducting back-to back audit processes, holding them in a constant state of audit, unnecessarily distracting security staff, and placing an increased burden on procuring agencies that will be required to renew the associated contracts yearly.

• Enabling application and registration to be accepted throughout the year, instead of on a quarterly basis. Allowing application and registration only four times a year could cause three-month delays or more for CSPs. Continuous application and registration throughout the year will enable ISMAP to keep pace with rapidly evolving cloud technology.

• Developing and appropriately resourcing a process for training an IT audit and certification workforce for cloud services in Japan, in parallel to the ISMAP development process.

• Emphasizing and ensuring the recognition of the shared responsibility model of cloud services[3]. We appreciate MIC for acknowledging this model in the draft Measures and would recommend MIC taking the lead in ensuring that this is understood across government agencies. Clearly incorporating the principle of shared responsibility into the ISMAP will ensure that the different responsibilities in cloud operations between CSPs and their customers regarding the establishment and maintenance of security controls to manage the risk to cloud services are recognized. It will also help clarify which entity is responsible for the aspects of the environment over which they have control and are accountable. This will avoid imposing security requirements or obligations on CSPs over customer data and systems to which they do not have access which can have counter-productive outcomes for security and privacy. For successful deployment, it is critical for cloud users and procurers to understand that they are required to minimize security risks by developing secure applications in the cloud environment as well as using tools and measures supplied by service providers as necessary, under their own responsibility.

• Recognizing third party, internationally accredited certifications and audit results as evidence of compliance with relevant ISMAP controls and requirements. This would reduce the need for on-site audits which are often impractical and expose the data centers to unnecessary physical security risks by requiring access to the site by otherwise unauthorized personnel.

We strongly encourage Japan's digital transformation (DX) objectives to be supported by cloud security policies that enable innovative, adaptable security approaches that

[3] https://cloudsecurityalliance.org/blog/2020/08/26/shared-responsibility-model-explained/

effectively leverage the security risk and resiliency benefits that cloud technologies provide.

In this respect, in addition to the review of ISMAP, we also recommend MIC to eliminate outdated security approaches, such as recommending to local governments in "Guidelines on Information Security Policies for Local Governments"[4] to carry out physical network separation of information systems that manage My Number data. While we fully understand and support the intention to protect citizen's privacy and personal information, such policies also create high costs for implementation, substantial barriers to the use of innovative cloud-based technologies and services which enable the use of this data as envisioned. Network separation, counterintuitively, may lead to systems becoming less secure.

Creating separate networks requires expenditures on building infrastructure that are necessary to support them such as standalone servers, routers, switches, management tools, etc. and reduces productivity and efficiency. Managing information between connected and separated networks and devices not only requires more time but can also lead to confusion and error which could lead to more security risks.

Many cloud services enable world class data security by implementing internationally recognized functions such as encryption and strict access management systems. The massive investments in data security of global CSPs, including those of many BSA members, provide the most effective data security for sensitive personal information available and it is imperative that the Government of Japan ensure that its policies enable the use of these best-in-class secure solutions. These best-in-class data security solutions adopt risk-based, outcome-oriented approaches[5]. They use security approaches such as zero-trust[6] security architectures, advanced user identity management and limited access systems, network controls such as always-on virtual private networks and virtual network segmentation, and strong data encryption in the data base layer in addition to the network layer, based on the "defense-in-depth"[7] approach.

As the concept of zero trust security architecture is to minimize "implicit trust zones" as much as possible, various security measures aligned with this concept need to be implemented, such as encrypting data to make it invisible even from the operator, as well as efforts to eliminate operational mistakes during the stage of design and development of systems. While these measures may appear peripheral to cybersecurity, they can be

[4] https://www.soumu.go.jp/main_content/000726079.pdf

[5] BSA International Cybersecurity Policy Framework
https://bsacybersecurity.bsa.org/report-item/bsa-international-cybersecurity-policy-framework

[6] Zero Trust Architecture, NIST SP-800-207
https://www.nist.gov/publications/zero-trust-architecture

[7] Defense-in-depth is defined by NIST as "the application of multiple countermeasures in a layered or stepwise manner to achieve security objectives……to ensure that attacks missed by one technology are caught by another." https://csrc.nist.gov/glossary/term/defense_in_depth https://www.ipa.go.jp/files/000056415.pdf

very effective approach to securing the entire IT system, including ensuring the security of network.

As such, we urge MIC to shift from outdated physical network separation and data localization requirements, and instead adopt security solutions tailored to current technologies, focusing on outcome-oriented risk management controls, and best practices based on the "defense-in-depth" principle to more effectively advance government operations through the acquisition and use of secure cloud computing services.

Cybersecurity solutions are most effective when they embrace public-private collaboration and foster market-driven solutions.[8] BSA and members look forward to working with MIC to promote the 'cloud by default' principle in both public and private sectors, including through working to improve ISMAP and providing educational sessions to raise awareness.

III Cross-sectional Measures
1. Promotion of Cooperation and Sharing of Cybersecurity Information Among Industry, Academia and Government

We fully agree with MIC's view that promoting the collection and analysis of information on cyber-attacks in collaboration with industry, academia and government will be critical for creating a safe cyber environment for digital reform and transformation. Encouraging voluntary data sharing arrangements can contribute to raising the level of security measures in the entire society. As cybersecurity threats are by nature global and not bound by national borders, useful threat intelligence on cyber-attacks requires sharing information across borders for effective analysis and research. This visibility can come from a range of sources, including customer install bases, published vulnerabilities, threat sharing networks, in addition to the options mentioned in the draft Measures such as sector-specific information sharing and analysis centers, such as(ISAC. The ability to source threat information globally for meaningful analysis does not depend on the physical location where threat research is conducted. Nor does enhancing cybersecurity depend on whether the technology deployed is domestic or foreign.

Domestic vendors in Japan, as with overseas operators, can undertake such research and derive actionable threat intelligence by drawing on threat information from worldwide sources, not just Japanese sources. Threat information sharing arrangements between domestic and foreign vendors can be an effective means to gather useful threat data to develop such domestic capabilities and avoid a "data loss spiral" described in the draft Measures. Many of BSA's members facilitate such intelligence sharing arrangements. We encourage MIC to strengthen information sharing and training for engineers in global scale, as well as focus on ensuring the adoption of best security technology available

[8] https://bsacybersecurity.bsa.org/report-item/bsa-international-cybersecurity-policy-framework

regardless of the country in which it is produced, to avoid the risk of Japan-unique cybersecurity model being disjointed from the rest of the world, which could hinder Japan's interest to lead cybersecurity internationally.

Conclusion

BSA hopes the above comments will be useful as you finalize the draft Measures. We support MIC's international leadership on cybersecurity matters to promote Data Free Flow with Trust (DFFT) and looks forward to collaborating with MIC to enhance cybersecurity to drive digital transformation in Japan. Please let us know if you have any questions or would like to discuss these comments in more detail.