BSA Comments on Draft Revised Guidelines on Information Security Policies in Local Governments

January 24, 2022

BSA | The Software Alliance (**BSA**)[1] welcomes the opportunity to provide our comments on the draft revised "Guidelines on Information Security Policies in Local Governments" (**Guidelines**) from the Ministry of Internal Affairs and Communications (**MIC**).

General Comments

BSA appreciates MIC's constant efforts to uniformly raise the level of cybersecurity in local governments. BSA members lead the world in offering cutting-edge technologies and services that support the digital transformation of governments and societies, including cloud computing, security solutions, data analytics, and artificial intelligence (**AI**). BSA works closely with governments around the world on the development of cybersecurity and data governance policies. We have witnessed first-hand the potential for such policies to effectively deter and manage cybersecurity threats while protecting the privacy and civil liberties of citizens.

The key elements for successful cybersecurity related polices include alignment with internationally recognized standards, adopting risk-based, outcome focused, technology neutral approaches, and developing adaptable policies to encourage innovation. Addressing cybersecurity challenges requires innovative tools and practices to defend the integrity, confidentiality, and resilience of the connected data ecosystem. It is important to be able to use the best available security solutions, including advanced encryption. We, therefore, encourage the Government to work closely with the private sector to develop security policies that benefit from the latest advancements in security approaches.

Observations and Recommendations

As Japan accelerates its efforts to realize the digital society, we are encouraged with the new Priority Policy Program (**Program**)[2] released recently from the Digital Agency. The Program presents the Government's firm commitment to modernize the information systems of local governments, recognizing the importance of maximizing secure cloud computing services for digital transformation. The pilot program for evaluating the "Government Cloud"[3] is currently underway in selected local governments. We strongly recommend that MIC, together with the

[1] BSA's members include: Adobe, Altium, Alteryx, Amazon Web Services, Atlassian, Autodesk, Aveva, Bentley Systems, Box, Cisco, CNC/Mastercam, CrowdStrike, 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] https://cio.go.jp/sites/default/files/uploads/documents/digital/20211224_policies_priority_package.pdf (Japanese) https://cio.go.jp/sites/default/files/uploads/documents/digital/20211224_en_priority_policy_program_01.pdf (English overview)

[3] https://www.digital.go.jp/policies/posts/gov_cloud (Japanese)

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

Digital Agency, continue updating the Guidelines with the view of expanding the use of public cloud to improve citizen services.

Promoting Cloud Use to Protect the My Number Network

We understand that the revised Guidelines are focused on creating an alignment with the recently updated "Common Standards for Cybersecurity Measures for Government Agencies and Related Agencies"[4] by the National Center of Incident Readiness and Strategy for Cybersecurity (NISC). We support the Guidelines' clarification that cloud services will be included under "external services", with security recommendations set based on the confidentiality of the information to be handled. We are also encouraged by the recognition of internationally recognized security standards and third-party audits for the selection of cloud services.

While we welcome these improvements to the Guidelines, we urge MIC to continue exploring security approaches that do not depend on the current three-tiered measures that may require physical network separation in some cases. BSA members' cloud services enable secure handling of sensitive personal information using internationally recognized functions such as encryption, zero-trust architecture, and advanced access management supported by the most secure infrastructure available in the world enabling reliable and safe access to services over the Internet. These cloud services provide the most effective data security solutions available to protect sensitive personal information and other data.

In line with this view, we urge MIC to revise the current approach to securing local government wide area networks (**LGWAN**) which can separate LGWAN from Internet-connected information systems. This physical separation prevents government organizations using the LGWAN from leveraging the advanced security and functionality of cloud computing. If helpful, we can help to organize technical sessions by BSA members to provide a better understanding of how security is provided under such Internet-connected configurations.

We fully support the need for local governments to safeguard information systems managing My Number data. However, public sector entities around the world are using cloud services for operations even, or especially, where information security is most required. Such organizations recognize the many benefits of high-quality cloud computing services including reliability, security, scalability and cost savings, speed, and ease of access and use. Cloud services offer the ability to innovate using AI, the Internet of Things (**IoT**), and other advanced technologies. We therefore encourage MIC to further update the Guidelines to ensure government agencies in Japan may access these benefits of cloud services.

Selection of Cloud Service Providers (CSPs) Should be Based on Data Security Practices and Not on Location

Further, we remain concerned that the explanation in the Guidelines relating to the use of external services appears to unnecessarily limit the use of CSPs that may store or process data in servers located outside of Japan. Ensuring data security depends on the technological and physical security controls maintained by the CSP. The location of the data center has very little to do with how CSPs protect personal information or comply with laws applicable to their users and customers. In fact, many of the advantages of cloud computing services derive from their ability to move data across international borders. Indeed, data security is improved by the resilience created by the ability to move and redundantly store data across multiple geographically dispersed data centers. This approach strongly aligns with "Data Free Flow with Trust" advocated by the Government of Japan. The Guidelines' focus on the physical location of data centers could lead to restrictions of such movement and may actually

[4] https://www.nisc.go.jp/active/general/pdf/kijyunr3.pdf (Japanese)

undermine the security of data handled by local governments. In consideration of the above, we respectfully request the MIC to modify the following section as follows:

> **Vol. 3: Information Security Policy in Local Governments (Explanation)**
> **Chapter 2: Standards for Information Security Measures (Explanation)**
> **8. Use of External Services**
> **8.2 Use of External Service (Upon Handling Information with Classification Level 2 or Higher)**
> **(2) Selection of External Services (Page iii-148)**
> When using external services that provide services via the Internet, it is necessary to note that the laws of the country where the data center is located may apply regardless of the location of the external service providers' place of business. Specifically, there is a possibility that information of a local government stored in an overseas data center through the use of an external service providers' services may be seized or analyzed by overseas authorities according to the laws and regulations of the country where the data center is located, even if such seizure or analysis is not permitted under Japanese laws and regulations. Therefore, it is necessary to select a data center that can be operated ~~**within the scope of Japanese laws and regulation**~~ **by a service provider that can provide assurances that data will be stored in a place and manner that allows the service provider to comply with Japanese laws and regulation**.

In addition, we note that section 8.2(2), paragraph 5 of the Guidelines recommends certain optional measures for local governments to assure themselves of the security of the external service provider, including by relying on audits or audit reports and certifications under various internationally recognized standards and other programs. These include ISO/IEC 27017 and the Information system Security Management and Assessment Program (ISMAP), and cloud information security audits of the Japan Security Audit Association and the Service Organization Control (SOC) Report. We welcome the flexibility that MIC is providing to local governments on the security assurances they can use. The Guidelines should state that the listed certifications, controls, and audit requirements are provided as alternatives for reference, and not all need to be met in order for local governments to base their decision when judging the reliability of the service and contractor. As such, we respectfully suggest the MIC to modify the relevant section as follows:

> **Vol. 3: Information Security Policy in Local Governments (Explanation)**
> **Chapter 2: Standards for Information Security Measures (Explanation)**
> **8. Use of External Services**
> **8.2 Use of External Service (Upon Handling Information with Classification Level 2 or Higher)**
> **(2) Selection of External Services (Page iii-149-150)**
> 5) The information security manager shall assess and judge comprehensively and objectively that the reliability of the external services and the contractors of the services is sufficient … In such an assessment, if the external service provider has obtained audit reports or certification by a third party that can be provided to users, the audit reports or certification shall be used. As for the certifications that will become selection condition, there is international standard for ISMS certification in the field of cloud services based on ISO/IEC 27017, and also, it is recommended to confirm that the ISMAP security controls are met and the ISMAP Cloud Service List, as well as cloud information security audit of the Japan Security Audit Association and the Service Organization Control (SOC) Report, which is an assurance report of internal control over security of external service providers. **One or more of the above may be used as a reference, and depending on individual cases, other appropriate certifications and security assurance may also be used**.

We also encourage this flexible approach on the security assurance requirements that external service providers are required to meet, as indicated in MIC's overview of the draft

revised Guidelines,[5] to be adopted by the central government. While recognizing that ISMAP is jointly administered by the National Center of Incident Readiness and Strategy for Cybersecurity (NISC), Digital Agency, Ministry of Economy, Trade and Industry (METI), and MIC, we encourage MIC to take the lead in providing the same flexibility of information security certifications for central ministries and agencies.

Modernizing Recommended Security Approaches Through Public-Private Partnership

We support the revised Guidelines addressing the increase in teleworking considering the security implications of the rapidly increasing availability and use of web-conference systems.

The Guidelines could further benefit from highlighting the countermeasures against increasingly frequent and consequential ransomware attacks. Various agencies and organizations have published information addressing efforts in this field,[6] and we recommend MIC make use of these references in the Guidelines.

We also strongly support robust partnership between government and industry to pursue consensus for cybersecurity actions. Cybersecurity solutions are most effective when they embrace public-private collaboration and foster market-driven solutions. BSA and our members look forward to working collaboratively with MIC to share insights into the latest advancement in security approaches.

Conclusion

BSA appreciates the opportunity to comment on the Guidelines. In the future, we strongly urge MIC to provide at least 30 days for comment to enable sufficient time for stakeholders to fully review and discuss the proposed approaches. We hope that our recommendations will be useful in completing the Guidelines and look forward to further supporting MIC to achieve Japan' digital transformation. Please let us know if you have any questions or would like to discuss comments in more details.

[5] https://www.soumu.go.jp/main_content/000785574.pdf (slide 10) (Japanese)

[6] https://security-portal.nisc.go.jp/stopransomware/(Japanese)