BSA Comments on Draft Guidelines on Information Security Policies for Local Governments (FY 2020)

December 22, 2020

BSA | The Software Alliance (**BSA**)[1] welcomes the opportunity to provide our comments on the "draft Guidelines on Information Security Policies for Local Governments (FY 2020)" (**Guidelines**) from the Ministry of Internal Affairs and Communications (**MIC**).

BSA is the leading advocate for the global software industry before governments and in the international marketplace. BSA members lead the world in offering cutting-edge technologies and services, including cloud computing, data analytics, machine learning, and artificial intelligence, collaborating with governments around to world to improve citizen services.

Observations and Recommendations

BSA appreciates MIC's constant efforts to improve information security measures for local governments. BSA has worked closely with governments around the world in relation to the development of cybersecurity policies and legislation. In doing so, we have witnessed first-hand the potential for such policies and legislation to effectively deter and manage cybersecurity threats whilst still protecting the privacy and civil liberties of citizens. We would like to provide the comments below to support MIC's effort to guide the security approaches of local governments.

Resolving Fragmentation of Information Systems Amongst Central and Local Governments

With Japan undergoing digital transformation under the leadership of the new administration to advance government operations, the acquisition and use of secure cloud computing services will be critical to achieve this endeavor. In this respect, we were encouraged that the review of the Guidelines has been conducted based on the "cloud-by-default" principle and presents new approaches enabling more Internet connectivity to support telework and improving the usability for government workers. The Guidelines would benefit from more explicit alignment with policies[2] developed by the Liaison Conference of CIO for the central government by promoting policies for "cloud native" architecture in local governments. Specifically, helping local governments to better evaluate the total costs of implementing LGWAN-based systems versus the total costs of cloud adoption would facilitate the local governments' transition to the cloud architecture.

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

[2] https://cio.go.jp/sites/default/files/uploads/documents/cloud_%20policy.pdf

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

Modernizing Recommended Security Approaches

MIC should review the traditional network security approach that relies on securing a perimeter, and instead, focus efforts on establishing principle-based guidelines for local governments that recommend baseline security/privacy responsibilities among various stakeholders, rather than prescribing specific security measures that local governments should adopt. We also recommend clarifying in the Guidelines that local governments have the autonomy to plan and execute information security policies that best serve the needs and risk profiles of their jurisdiction.

In addition, we recommend revising the guidance described in Part 3, Chapter 2, Section 4.1 (7) Destruction of Equipment, which provides prescriptive measures on the disposal of devices that store personal information of citizens. Requirements for physical destruction of storage devices and on-site monitoring of the process by local government officials presume on-premises IT systems. To accommodate innovative uses of cloud computing by local governments, the Guidelines should focus on making data unrecoverable when no longer in use, rather than prescribing a detailed media or data destruction method. Accordingly, we recommend clearly identifying mechanisms that make data unrecoverable by acknowledging data deletion methods such as cryptographic erase.

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

While we welcome the review of the Guidelines based on the “cloud-by-default” principle, we remain concerned that the explanation in the Guidelines relating to the use of cloud computing services appears to 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 users. In fact, many of the advantages of cloud computing services derive from the 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 as the key underlying concept of the G20 Osaka Track. As such, the Guideline’s focus on the physical location could lead to restrictions of such movement and may actually undermine security for the 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 Service 8.4 Use of cloud service**
> **8.4. Use of Cloud Service (Page iii-142)**
>
> (2) When using cloud 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 cloud service provider's office. Specifically, there is a possibility that information of a local government stored in an overseas data center through the use of a cloud service provider's service 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, when storing highly confidential information such as resident information, 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. There should also be consideration made on having a data center**

for backup overseas from the viewpoint of data preservation, disaster control measures, etc.

Promoting Cloud Use to Protect the My Number Network

While fully encouraging the need to safeguard information systems managing My Number data, we recommend MIC to continue exploring security approaches and guidance that do not deter the adoption of cloud computing solutions by local governments or unnecessarily undermine their benefits. Cloud services enable secure handling of sensitive personal information, utilizing internationally recognized functions such as encryption and storage management, while building a system under the most secure global infrastructure. The ever-evolving nature of cloud services will provide the most effective data security to protect sensitive personal information.[3]In line with this view, we also urge MIC to revise the current approach on LGWAN and not divide LGWAN and Internet-connected information systems to leverage such features of cloud.

Adopt Latest Approaches to Security Through Embracing Public-Private Sector Collaboration

As noted above, security approaches are evolving rapidly reflecting technological advancement. Best practices for data security adopt risk-based, security outcome-oriented, defense-in-depth and zero-trust security architecture approaches such as advanced user ID management and limited access, network controls such as always-on secure virtual private networks and network segmentation, and implementation of strong data encryption. We encourage MIC to continue reviewing the Guidelines in the future, to adopt security solutions better tailored to current technologies, focusing less on prescriptive requirements and more on outcome-focused risk managed 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.

We also strongly support robust partnership of government and industry to pursue international consensus for cybersecurity actions and were encouraged to see MIC’s recognition of ISO and SOC standards in the Guidelines as the bases for evaluating cloud security. 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 would encourage 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 recommendation will be useful in completing the Guidelines and look forward to further supporting MIC to achieve Japan’s digital transformation. Please let us know if you have any questions or would like to discuss comments in more details.

[3] https://cio.go.jp/sites/default/files/uploads/documents/dp2020_03.pdf