"Guidelines on Information Security Policies in Local Governments" (FY 2018)

Comments of BSA | The Software Alliance

July 27, 2018

BSA | The Software Alliance ("**BSA**")[1] welcomes this opportunity to provide our comments on the draft *Guidelines on Information Security Policies in Local Governments (FY 2018)* ("**Guidelines**"), published by the Ministry of Internal Affairs and Communications ("**MIC**") on July 17, 2018, 2018.

BSA appreciates the Government of Japan's ("**GOJ**") commitment to improving the information security measures utilized by the central government agencies and local governments by revising the *Common Standards for Information Security Measures for Government Agencies* ("**Common Standards**") and the Guidelines.

Summary of BSA Recommendations:

[1] BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 60 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.

BSA's members include: Adobe, Amazon Web Services, ANSYS, Apple, Autodesk, AVEVA, Bentley Systems, Box, CA Technologies, Cadence, Cisco, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, SAS Institute, Siemens PLM Software, Splunk, Symantec, Trend Micro, Trimble Solutions Corporation, and Workday.

We urge MIC to revise the Guidelines to explicitly support the adoption of cloud computing services by local governments, in line with the GOJ's goal of promoting Digital Government. Specifically, we recommend that MIC:

- Remove or revise recommendations to specify or restrict where data may reside to ensure that cloud service providers (**"CSP"**) can utilize regional and global infrastructure to store and process data.
- Eliminate recommendations to physical separate networks from the Internet, so that local governments may be able to utilize cloud services in providing enhanced e-government services to residents.
- Explicitly acknowledge the autonomy of local governments to select the best IT solutions and information security approaches based on commercially negotiated cloud services agreements to fit their needs, and to encourage active information sharing to spread the adoption of best practices.

Introduction:

Japan is strongly promoting the concept of Digital Government in response to the increasingly digital society, by fully utilizing information technology (**"IT"**), improving the convenience, efficiency, and transparency of government administration, and reviewing administrative services. Local governments which provide public services directly to citizens are expected to effectively utilize IT to provide better public services while meeting the changing needs of citizens in a cost-effective way, while concurrently protecting the citizens' privacy.

BSA has established a forum for industry, government, and academia to work together to discuss best practices to achieve these goals. During discussions in the forum, we have come to following understandings:[2]

[2] Information regarding the forum can be found at http://bsa.or.jp/news-and-events/news/bsa20180420/ and https://bsa.or.jp/news-and-events/news/bsa20170413_2/

1. Central and local governments are all highly interested in providing public services in an improved fashion, and it is essential to utilize cloud services and other new technologies to achieve this aim;
2. Assuring security for citizens' information is critically important to nurture trust and accountability and it is also vital to continue to adopt approaches that are consistent with technological advancements; and
3. Providing flexible guidance which enables mobility and choice of services and autonomy enables local governments to make the best choices for citizens.

BSA Recommendations:

Promote the Cloud-by-Default Principle

Cloud computing is a critical enabler of innovation across all industries. Laws, regulations, and policies related to cloud services should support and accelerate the spread of cloud services. Recognizing this, the GOJ recently announced the *Basic Policy on Use of Cloud Services in Government Information Systems* (the "**Basic Policy**") and described that the government information systems should consider cloud services as the first option (i.e., the "Cloud-by-Default Principle"). BSA supports this principle and recommends that MIC also promote the Cloud-by-Default Principle in the Guidelines.

Avoid Requirements for Data Localization

Furthermore, in order to maximize the benefits of cloud computing services, including economies of scale and cost benefits, redundancy for back-up, and real-time updates of systems in response to global cybersecurity threats, it is vital to optimize and ensure smooth cross-border data transfers on a global scale.

To that end, we urge clarifications to "(Note 7) Considerations for Use of Cloud Services" (iii - 117) in the Guidelines, which imposes limitations on the use of foreign servers. The location of the data center has very little to do with whether and how CSPs protect personal information or comply with laws applicable to users. Data security does not ultimately depend on the physical location of the data. Rather, it is a quality of functionality, effectiveness of mechanisms, and the controls maintained to protect the data. It is not necessary to specify the particular location where data resides, as long as the CSP can ensure that the data will be handled securely and appropriately and in accordance with the governing laws. Many of the advantages of cloud computing services derive from the mobility of data across international borders. Thus, imposing requirements which tend to restrict such movement or require accounting for the "physical location" of data may limit the adoption of cloud computing services by local governments without adding any additional security to their data.

In consideration of the above, we respectfully request the MIC to modify the following accordingly:

"(Note 7) Consideration for Use of Cloud Services" (page iii-117)

When using cloud services which are provided over the Internet, special attention should be paid to the laws of the country in which the data center is located, regardless of the location of the business office of the cloud service provider. Specifically, there is a possibility that information of local governments stored in data centers outside Japan through the use of services provided by cloud service providers may be seized or analyzed by foreign authorities based on the laws of that country, even if such conduct is not permitted under Japanese laws. Therefore, when highly sensitive information such as resident information will be stored, it is necessary to select a data center that ~~**can be operated within the scope of Japanese laws and regulations**~~ **is located in a jurisdiction with robust rule of law mechanisms and operated by a service provider that can provide assurances that data will be stored in a manner that is consistent with Japanese laws and regulations**."

Eliminate Recommendations to Physically Separate Networks

We are concerned that pages ii-6, ii-7, and iii-10 of the Guidelines propose the physical separation of the telecommunications network between the business systems which connect to the Local Government Wide Area Network (**"LGWAN"**) and the information systems which connect to the Internet as an information security measure. In general, physical separation of networks is a very costly endeavor and significantly reduces the ability to access and utilize the information held in such systems. Systems must communicate with each other in order to be of genuine use, and physical network separation interferes with this functionality.

Physically separating systems from the Internet also reduces the real-time and widescale security benefits of a cloud deployment, preventing CSPs from providing patches and active threat intelligence in a timely manner. Physical separation can also introduce new security gaps as low security-conscious personnel to try to bypass the inconveniences of such separated systems.

A multi-layered approach to cybersecurity can provide effective protection against threats whereas attempting to physically separate systems from the Internet may grant only illusory security benefits and undermine the productivity gains which cloud services can provide. This represents a fundamental concept of information security referred to as “defense-in-depth”. Cutting an information system off from the Internet not only limits the accessibility and usability of any relevant data, but it also limits the government agency concerned from benefiting from the cutting-edge security solutions employed by leading CSPs.

Therefore, we recommend MIC delete the descriptions on pages ii-6, ii-7, and iii-10, and the relevant pages regarding the physical separation of the telecommunications network between the business systems which connect to the LGWAN and the information systems which connect to the Internet. This will help prevent the Guidelines from misleading local government officials into inferring that the most effective way to ensure the security of information systems is to attempt to isolate them from the Internet.

If eliminating the section’s referencing physical network separation is not feasible at this stage, we urge MIC to at least clearly state that risks are not determined solely by whether the information system is connected to the Internet. We refer MIC to Page 5 of the Basic Policy, which states that the security of an information system should not be determined solely by the presence or absence of connection to the Internet and it should not be assumed that cloud services are dangerous simply because they are connected to the Internet. We are in full agreement with this sensible view.

Encourage the Autonomy of Local Governments and Provide Flexible Guidance

The autonomy of each local government should be actively reflected in the Guidelines, and the adoption of best practices by local governments in accordance with technological advancements should not be hindered through the enforcement of an information policy such as uniform physical network separation.

Page i-10 of the Guidelines states that "the information security policy should be prepared by local governments on their own initiative in accordance with the actual conditions of the organization since information security in local governments should be ensured at their own responsibility in protecting information assets held by local governments" and "the composition and examples described in the Guidelines are provided as a reference and do not preclude local governments from defining information security policies by their own composition and expression." We agree with this idea. Local governments should have the flexibility to develop the information security measures they require and ensure their CSPs to implement these requirements by including them in commercially negotiated cloud services agreements.

As technology advances and the social situation changes day to day, we hope that leading local governments will share their efforts on information security and IT governance with other local governments, that best practices will be adopted among such local governments, and that this will create a virtuous circle for achieving digital government for providing improved public services to citizens.

Conclusion:

BSA appreciates this opportunity to comment on the Guidelines. Although the period between publishing the draft Guidelines and the end of the comment period, only ten days, was far too short and we encourage MIC to provide at least 30 days for comment in the future, we hope that our observations and recommendations set forth above will be useful in completing the Guidelines. Furthermore, we hope that they will be useful in continuing the government's activities to promote the adoption of cloud services and other new technologies, which are effective measures for improving cybersecurity capabilities of information systems in local governments, providing superior and more efficient public services, and solve social challenges. Please let us know if you have any questions or would like to discuss these comments in more detail.

-End-