Recommendations from BSA | The Software Alliance on Japan's Digital Transformation

October 1, 2021

BSA | The Software Alliance (**BSA**)[1] congratulates the Government of Japan on the establishment of the Digital Agency (**Agency**) which functions as the control tower for the formation of a digital society, with the goal of establishing public-private infrastructure for the digital age in a citizen-centric manner. BSA and our members work closely with governments around the world to improve citizen services and look forward to collaborating with the Agency to support the various initiatives to be undertaken in the future.

BSA is the leading advocate for the global software industry before governments and in the international marketplace. BSA's members are at the forefront of the data-driven innovation that is fueling global economic growth and recovery, including through cutting-edge advancements in cloud computing, security solutions, artificial intelligence (**AI**) and machine learning, and the Internet of Things (**IoT**). BSA members provide software solutions to enterprise customers and their business models do not depend on monetizing the data of their customers. In fact, they often provide tools to facilitate their customers' compliance, such as on privacy and cybersecurity. In Japan, these enterprise software companies support a wide range of organizations, including SMEs and large companies; local and central governments; hospitals, schools, universities, and non-profits, contributing to Government's ongoing digital transformation efforts.

With the release of Priority Policy Program,[2] BSA and BSA members were encouraged to learn that the Agency will be putting focus on facilitating data utilization across ministries to improve citizen services. Taking a unified approach to updating central and local government information systems and websites, facilitating data linkage in medical, education, and disaster management sectors, and working to ensure trust of data through improvement of verification mechanisms are important objectives that we fully support. These important programs will create a resilient society and we look forward to continuing to explore ways to collaborate with you to drive these initiatives to enable public sector entities to benefit from cutting edge technologies available in the global marketplace.

As acquisition and use of secure cloud computing services will be critical to achieve these goals, BSA offers the below recommendations to support the Agency's priorities.

[1]BSA's members include: Adobe, Altium, Amazon Web Services, Atlassian, Autodesk, 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., Splunk, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, Workday, Zendesk and Zoom.

[2] https://cio.go.jp/sites/default/files/uploads/documents/digital/20210901_en_04.pdf
http://www.kantei.go.jp/jp/singi/it2/kettei/pdf/20210615/siryou6.pdf (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

Observations and Recommendations

Continuous improvement of Information system Security Management and Assessment Program (ISMAP) to Successfully Drive Cloud Computing Uptake in Digital Society

BSA welcomes the Agency's focus to ensure the "cloud-by default" principle to be implemented across the public sector and that discussions are underway to establish the Government Cloud, an environment enabling the use of multiple cloud services (IaaS, PaaS, SaaS) that provides a common infrastructure and functions for government information systems. We are also encouraged that further improvement is being considered for the existing Information system Security Management and Assessment Program (**ISMAP**), which will be the basis for driving this initiative. We fully support such efforts as the current ISMAP is placing significant compliance burdens and prohibitive costs on cloud service providers (**CSPs**) wishing to be registered on the ISMAP Cloud Service List. To drive further cloud uptake, we recommend the Agency work with relevant ministries and affected industry stakeholders to improve ISMAP by focusing on the following:

- Emphasizing and ensuring the recognition of the **shared responsibility** model of cloud services.[3] For the successful deployment of cloud computing, it is critical that cloud users and procurers understand that they are required to minimize security risks by developing secure applications in the cloud environment as well as by using tools and measures supplied by CSPs as necessary. Clearly incorporating the principle of shared responsibility in ISMAP will ensure that the different responsibilities for cloud operations between CSPs and their customers to establish and maintain 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, and not for those over which they have no visibility. This will avoid imposing security requirements or obligations on CSPs over customer data and systems to which they do not have access, and which can consequently have counter-productive outcomes for security and privacy if they are subject to inappropriate obligations.

- Making 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 risks most relevant to these respective services.

- Reducing repetitive auditing process by exempting the application of security controls that are duplicative with internationally recognized standards for which certification have already been received. Given that many CSPs already have internationally accredited certifications (ISMS-JISQ/ISO 27000 series), acknowledging them and eliminating repetitive procedures and requirements to reuse evidence already provided in prior certifications from ISMAP will contribute to alleviating the burden of all stakeholders involved, including the Government of Japan. This will also lead to facilitating more companies in Japan to be ISMS/ISO certified and to actively utilize such certifications, opening them up to greater international business opportunities.

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

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

- Increasing the number of auditing firms registered under ISMAP will enable flexible choice for CSPs. In order to avoid concentration and lack of resources to fulfill current and future demands for audit procedures required under ISMAP, we strongly recommend reviewing ways to facilitate more auditing firms to be registered under ISMAP. This will enable fair competition between auditing firms and will provide CSPs a wider variety of choices, rather than being forced to choose from only the existing four registered firms. In parallel, developing and appropriately resourcing a process for training an IT audit and certification workforce for cloud services will be important to make ISMAP sustainable.

- Further, establishing a less frequent auditing schedule in line with international cloud security best practice (e.g., once every three years) will reduce the audit overheads to CSPs and the Government of Japan alike. Yearly audits could result in CSPs conducting effectively 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 seeking ISMAP registration. Continuous application and registration throughout the year will enable ISMAP to keep pace with rapidly evolving cloud technology.

Promoting Adoption of the Most Effective Security Approaches Reflecting the Latest Technologies

We understand that the Agency will be working to unify and standardize systems including backbone systems of local governments, to be constructed on the Government Cloud. We look forward to the development of this initiative, which is expected to drive effective utilization of data held at municipalities. For local governments to truly benefit from the use of innovative cloud-based technologies and services to enable the use of data as envisioned, we strongly urge the Agency to work with Ministry of Internal Affairs and Communication (MIC) to review and update the existing Guidelines for Information Security Policies for Local Governments (**Guidelines**).[4] These Guidelines continue to include a three-tiered security approach recommending physical network separation. While we fully support the objective of protecting citizens' privacy and personal information, maintaining such outdated policies deters public sector entities from adopting cloud computing solutions and are not in proportion to the risk to the data. In fact, the 3rd Edition of "Guidelines for Information Security Measures for the Provision of Cloud Service" which MIC has recently put up for public consultation takes into consideration multi-cloud infrastructure and the shared responsibility model, in anticipation of the constantly evolving cloud technology environment and the increasingly complex digital platform landscape. As such, we request the Agency to coordinate policies to reflect the latest technological advancement.

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 by 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 Agency ensure that its policies enable the use of these best-in-class secure solutions.

[4] https://www.soumu.go.jp/main_content/000727474.pdf

These best-in-class data security solutions adopt risk-based, outcome-oriented approaches.[5] They use security approaches such as zero-trust security architectures,[6] 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. As such, the Agency should work with MIC to eliminate outdated physical network separation requirements 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[7] to more effectively advance government operations through the acquisition and use of secure cloud computing services. Doing so would help build a flexible and robust foundation for the Government Cloud in Japan. Governments[8] that have adopted these critical practices have been successful in making the most effective use of cloud computing while more effectively countering dynamic cyberthreats.

Cybersecurity solutions are most effective when they embrace public-private collaboration and foster market-driven solutions.[9] BSA and our members look forward to working collaboratively with the Agency to ensure Japan's digital transformation and security policies benefit from the latest advancements in security approaches.

Private and Public Sector Collaboration to Improve Digital Skills of the Public Sector

We also welcome the Agency's strong focus on enhancing digital talent training in the public and private sectors. To fully embrace the potential of today's technology, we encourage the Agency take advantage of various training opportunities offered by BSA members[10] to support its efforts to improve the digital skills of the public sector workforce and to build the Government's data science capabilities, as well as promote such efforts in the private sector.

Further, we encourage the Digital Agency to establish a formal process or mechanism in which IT industry stakeholders can actively participate in periodic discussions to develop, refine, and implement digital transformation policies and strategies. Enabling open and transparent processes will be the key to ensuring the Agency's success in achieving digital transformation and such a collaborative forum with the private sector will enable the Agency to benefit from the up-to-date expertise and best practices of industry representatives.

---

[5] BSA International Cybersecurity Policy Framework at 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

[8] US: https://cloud.cio.gov/strategy/
UK: https://www.gov.uk/guidance/creating-and-implementing-a-cloud-hosting-strategy

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

[10] Training Opportunities:
https://transformyourtrade.org/training-opportunities/
https://bsa.or.jp/policy/digitalskill/ (Japanese)

Conclusion

BSA looks forward to the opportunity to have wide range of conversation on how BSA and our members can work together with the Agency to facilitate digital transformation and generate value for government investment in services provided by the private sector.

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