Comments from BSA | The Software Alliance
on the Formulation of the New Priority Policy Program

November 18, 2021

BSA | The Software Alliance (**BSA**)[1] welcomes the opportunity to provide comments to the Digital Agency (**Agency**) for the formulation of the new Priority Policy Program (**Program**).

BSA is the leading advocate for the global software industry before governments and in the international marketplace. Our members are at the forefront of the data-driven innovation fueling global economic growth and recovery. They create the technology products and services that empower governments and other businesses, offering tools such as cloud storage services, customer relationship management software, human resource management programs, identity management services, collaboration software, electronic signatures, and security solutions. 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 the Government of Japan's ongoing digital transformation efforts.

BSA works with governments around the world to facilitate digital transformation, and based on the experiences gained, provides the below comments in response to the questions raised from the Agency.

1. What kind of digitalization will be necessary to achieve economic growth?
(1) Digitalization Through Cloud
We support the Government of Japan's adoption of the "cloud-by-default principle" in the public sector. This policy correctly recognizes that the implementation of modern cloud-based software solutions is the key driver for digital transformation and achieving economic growth.

Cloud solutions can improve the quality of services, strengthen cybersecurity, and increase the versatility and resiliency of organizations and their workforces in both public and private sectors.

We were encouraged that the Government of Japan took steps to establish the Information system Security Management and Assessment Program (**ISMAP)**, designed to enable the smooth adoption of cloud services across government agencies. However, we are now concerned that the current ISMAP controls and requirements are not sufficiently aligned with internationally recognized standards and that the process of ISMAP certification does not adequately recognize the validity certification to such standards. Requiring companies seeking registration on the ISMAP Cloud Service List to separately demonstrate compliance with ISMAP controls to which they are already certified under other widely accepted security

---

[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, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

standards represents a significant burden and cost on cloud service providers (**CSPs**). This will also strain the resources of the Government of Japan as it implements the ISMAP, delaying certification of otherwise eligible cloud services.

We support the goal of ISMAP to encourage cloud adoption in the public sector by enhancing transparency, consistency, and trust in the security of cloud computing services. Unfortunately, the compliance challenges described above could lead to some providers of secure and trusted cloud services to refrain from seeking ISMAP registration — including those that have demonstrated compliance with internationally recognized security standards. This will result in fewer options and less competition without improving security.

As such, we **strongly recommend** the Agency include a review of ISMAP in the new Program with the stated goal of improving the system. This review should involve close consultation with relevant ministries and affected industry stakeholders.[2] Establishing a mechanism that fully leverages internationally recognized standards (e.g., recognizing certification to the ISMS-JISQ/ISO 27000 series as satisfying relevant ISMAP requirements) will alleviate the burden of all stakeholders involved, including the Government of Japan. Such an approach 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 and promoting economic growth.

We understand that, while the procurement of cloud services using ISMAP is currently only a requirement for government agencies, the Government expects the private sector to refer to the registered ISMAP cloud services when making their own purchasing decisions.[3] While we welcome the intention of the Government to play a leading role in the adoption of advanced technologies to incentivize private companies that are yet to fully leverage the benefit of cloud, we urge the Government of Japan to refrain from encouraging Japan's private sector enterprises to refer to ISMAP certified cloud services for their acquisition of cloud computing services until the challenges described above are addressed.

(2) Leveraging Digital Tools
One effective solution for driving economic growth through digitalization is to facilitate the use of digital tools, including advanced data analytics, remote collaboration tools, and the legal and commercial adoption of electronic signatures that are compatible with services widely used around the world. More than ever before, economic growth in Japan relies on companies of all sizes operating internationally to be able to move at increasing speeds in an electronically connected global economy.

In this regard, we are encouraged that the Government of Japan has taken steps to shift to paperless transactions and to decrease long-standing hanko seals requirements for administrative procedures, as well as clearly indicating the objective to "spread e-signature, e-proxy and e-certificate of commercial registration" in the earlier Program.[4]

However, we continue to see reliance on physical paper and hanko seals for parties to indicate their intention to be bound to a legal agreement or to interact with government bodies. As such, we **recommend** the Agency facilitate more comprehensive use of electronic signatures to allow Japanese and foreign businesses to carry out transactions quickly and securely from any location in the world, and we **recommend** the Agency reflect this in the new Program.

---

[2] https://www.bsa.org/files/policy-filings/en10012021reccjapandigitransform.pdf

[3] https://www.nisc.go.jp/active/general/ismap.html

[4] Priority Policy Program for the Realization of a Digital Society (Overview), page 2, https://cio.go.jp/sites/default/files/uploads/documents/digital/20210901_en_04.pdf

Another important factor to drive economic growth is facilitating international data transfers. Among other things, this allows both the public and private sectors to leverage best-in-class technology globally. As stated in the earlier Program, we look forward to Japan's continued leadership in driving Data Free Flow with Trust (DFFT) and promoting cross-border data transfers internationally and encourage the Agency to discourage domestic preferences for data localization.

(3) Improving Security of Digital Tools
Improving the security of digital tools through ensuring software is developed and deployed using best practices is more important than ever. To support stakeholders in the software industry — developers, vendors, customers, policymakers, and others — to communicate and evaluate security outcomes associated with specific software products and services, BSA developed a standards-based risk management tool, "The BSA Framework for Secure Software" (**Framework**).[5] This Framework is intended to be used to: (1) help software development organizations describe the current state and target state of software security in individual software security products and services; (2) help software development organizations identify opportunities for improvement in development and lifecycle management processes, and assess progress toward target states; (3) help software developers, vendors, and customers communicate internally and externally about software security; and (4) help software customers evaluate and compare the security of individual software products and services. The Framework is intended to focus on software products (including Software-as-a-Service) by considering both the processes by which a software development organization develops and manages software products and the security capabilities of those products. It is intended to complement guidance for overall organizational risk management processes. To the greatest extent possible, the Framework seeks alignment with internationally recognized standards and is intended to remain flexible, adaptable, outcome-focused, and risk-based. We therefore **encourage** the Agency to leverage the Framework to improve the security of the digital tools essential for economic growth.

(4) Promoting Utilization and Responsible Governance of AI
Artificial intelligence (AI) and machine learning (ML) are also key drivers of economic growth. The ability to digest large quantities of data has been a critical component of improving business operations and efficiencies, and many leading software companies have been quick to develop various AI-powered technologies. We are encouraged that the Government of Japan has acknowledged the benefits of AI, developing a comprehensive strategy[6] with a clear objective for Japan to become a frontrunner in the application of AI in industry to strengthen global competitiveness. To support this goal and to promote further AI utilization, organizations designing and deploying AI systems should do so in ways that account for the potential risks of unintended bias that may arise, particularly in high-risk use cases. Like cybersecurity and privacy, managing the risks of AI bias requires an organizational commitment that extends throughout a system's lifecycle.

To support such efforts, BSA has developed "BSA's Framework to Build Trust in AI" (**AI Framework**)[7] as a tool to ensure that AI is accountable by design. The AI Framework can be used by organizations of all types to manage the risk of bias throughout a system's lifecycle. This Framework: 1) outlines a process for performing impact assessments to identify and mitigate potential risks of bias, 2) identifies existing best practices, technical tools, and resources for mitigating specific AI bias risks that can emerge throughout an AI system's

---

[5] https://www.bsa.org/files/reports/bsa_framework_secure_software_update_2020.pdf

[6] AI Strategy 2019 at https://www8.cao.go.jp/cstp/ai/aistratagy2019en.pdf and AI Strategy 2021 (follow-up of AI Strategy 2019) at https://www8.cao.go.jp/cstp/ai/aistrategy2021_honbun.pdf

[7] https://ai.bsa.org/confronting-bias-bsas-framework-to-build-trust-in-ai

lifecycle, and 3) sets out key corporate governance structures, processes, and safeguards that are needed to implement and support an effective AI risk management program. Organizations can use this Framework to enhance trust in their AI systems through risk management processes that promote fairness, transparency, and accountability. As AI is used in ways that will have increasingly consequential impacts on people's lives, we **strongly recommend** the Agency and industry leaders to align around best practices for mitigating the potential risks of AI bias.

2. Please share your experience on digital governments outside of Japan.
While we applaud the Agency's speedy digital transformation efforts, we also recommend establishing a system to evaluate and monitor the service indicators associated with digitalization, including surveys of public satisfaction with these indicators. The European eGovernment Benchmark (**Benchmark**),[8] which is a survey conducted annually by the European Commission to assess the state of eGovernment in European countries, is good example of such a system. The aim of the Benchmark is to promote competition between Member States and to increase the benefits of e-government for the European population. The Benchmark evaluates each country on the following four indicators: 1) User centricity: How well are services provided online? Are they mobile-friendly? What online support and feedback mechanisms are in place? 2) Transparency: Does the public administration provide clear and openly communicated information on how services are provided? Are public authorities transparent about their responsibilities, their performance, and how they process people's personal data? 3) Cross-border mobility: How easy is it for citizens abroad to access and use online services? 4) Key enablers: What technical enablers are in place for the provision of e-government services?

BSA member company Adobe conducted a global survey[9] covering seven countries and over 7,000 citizens to better understand the factors that contribute to positive experiences with online public services. The research indicated that positive experiences with eGovernment correlate with the combination of five factors: 1) facilitating the citizens journey to engage with eGovernment to meet their needs; 2) providing services optimized for mobile devices such as tablets and smartphones; 3) designing graphics, visuals, and content to work together in a seamless and meaningful manner; 4) ensuring that the services provided and that are highlighted are relevant to the needs of citizens; and 5) establishing a relationship between the citizens and their government, assisting citizens to evolve from passive recipients of content to becoming co-creators of ever more relevant services.

Conducting similar surveys in Japan would provide invaluable feedback about the public's expectations and assessment of the Government of Japan's progress in driving effective eGovernment.

3. What will be necessary to secure and nurture "digital workforce/talent"?
We 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.

---

[8] https://digital-strategy.ec.europa.eu/en/library/egovernment-benchmark-2020-egovernment-works-people

[9] Delivering experiences that count: Global survey results and insights on digital citizen services at https://landing.adobe.com/dam/2017/downloads/whitepapers/ctir-2798.en.delivering-experiences-that-count.pdf and https://landing.adobe.com/en/na/solutions/government/ctir-2798-wpp-adobe-global-citizen-benchmark.html

[10] Digital Skills Training Programs: https://bsa.or.jp/policy/digitalskill/
Training Opportunities: https://transformyourtrade.org/training-opportunities/

4. What do you expect from "digitalization of daily life"?

In cooperation with the private sector, "digitalization of daily life" should reduce the burdens of individuals, making it easier for citizens to conduct business with the government and with each other. To achieve these outcomes, it is important to promote coherence (standardization and interoperability) between different levels of the public sector. We understand that the Agency has set a goal of promoting standardization and collaboration of local government information systems by 2025. However, due to a lack of staff and knowledge, some small and medium-sized local governments are unlikely to be able to achieve these goals on their own. Therefore, the Agency may need to facilitate coordination and joint investments among small government entities to enable the deployment of common digitally enabled systems and services. We encourage the Agency to look to the expertise of BSA members in supporting such efforts, given their experience with contributing to the digitalization efforts of governments across the globe, including in response to COVID-19 which has enabled research and safe distribution of vaccine.[11]

5. What do you expect from the "digitalization of local region"?

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, with pilot programs running in selected municipalities. We look forward to the development of this initiative, which is expected to drive digitalization of local regions and enabling local governments to more effectively use data they hold. For local governments to truly benefit from the use of innovative cloud-based technologies and services, we **strongly urge** the Agency, based on the result of these pilot programs and working with Ministry of Internal Affairs and Communication (**MIC**), to update the existing Guidelines for Information Security Policies for Local Governments **(Guidelines),**[12] including revising the three-tiered security approach to eliminate recommendations for physical network separation.

We fully support the objective of protecting citizens' privacy and personal information, but maintaining such outdated policies deters public sector entities from adopting cloud computing solutions, may undermine instead of enhance data security, and are not in proportion to the risk to the data. In anticipation of the constantly evolving cloud technology environment and the increasingly complex digital platform landscape, we instead **recommend** the Agency to coordinate policies to advance the adoption of multi-cloud infrastructure and a recognition of the shared responsibility model, as described in MIC's 3rd Edition of "Guidelines for Information Security Measures for the Provision of Cloud Service"[13], as a priority focus in the new Program.

Many BSA members provide best-in-class data security solutions, adopting risk-based, outcome-oriented approaches.[14] They use security approaches such as zero-trust security architectures,[15] 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 focus on adopting security solutions tailored to current technologies, focusing on outcome-oriented risk management controls, and

---

[11] https://software.org/news/covid-19-response-software-vaccine-research-security-distribution/

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

[13] https://www.soumu.go.jp/main_content/000771515.pdf

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

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

best practices based on the "defense in depth" principle[16] to more effectively advance government operations through the acquisition and use of secure cloud computing services and to facilitate digitalization of local region.

6. What is your view on "people-friendly digitalization in which no one is left behind"?
In order to address the issue of the digital divide for the elderly and other informationally vulnerable people, we agree with the Agency that there should be a focus on digital inclusion. BSA welcomes working with a dedicated department within the Agency to respond to this issue and would welcome the opportunity to discuss how the industry could assist in this effort.

Conclusion

BSA looks forward to the opportunity to have wide range of conversation on how BSA can work together with the Agency to facilitate digital transformation and generate value for government investment in services provided by the private sector. Please let us know if you have any questions or would like to discuss these comments in more detail.

---

[16] 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