Comments from BSA | The Software Alliance on Cloud Service Registration Rules, etc. (Draft) of Information system Security Management and Assessment Program for Low-Impact Use (ISMAP-LIU)

July 5, 2022

BSA | The Software Alliance (**BSA**)[1] welcomes the ongoing efforts of the National center for Incident readiness and Strategy for Cybersecurity (**NISC**), the Ministry of Economy, Trade and Industry (**METI**), the Ministry of Internal Affairs and Communications (**MIC**), and the Digital Agency (**relevant agencies**) to accelerate digital transformation across the government. Our comments relate to the relevant agencies efforts to establish the "Information system Security Management and Assessment Program for Low-Impact Use (**ISMAP-LIU**)" designed to promote the adoption of low-risk software-as-a-service (**SaaS**) cloud computing by government agencies.

General Comments

BSA is the leading advocate for the global software industry before governments and in the international marketplace. Our members lead the world in offering cutting-edge cloud computing technologies and services that can help governments be more nimble, productive, and innovative while also improving network security and system availability. Based on our experiences with cloud security assessment programs in other markets, we provide the following recommendations to support the government's goal of implementing the "cloud by default" principle.

Observations and Recommendations

As the relevant agencies recognize, SaaS provides a wide range of services, including those that handle only low-critical information among confidentiality class-2 information. By designing a cloud security assessment mechanism that avoids excessive compliance requirements, the government may further promote utilization of these services by the public sector in Japan.

Some of the proposed modifications for ISMAP-LIU, such as reducing the number of controls subject to external audits and requiring annual internal audit report to cover the entire control objectives in three-year cycle, may prove helpful in facilitating public sector cloud adoption. In fact, applying such changes to ISMAP itself would be very beneficial.

However, the proposed ISMAP-LIU would better achieve the relevant agencies' goals by adopting the following recommendations.

[1] BSA's members include: Adobe, Alteryx, Altium, Amazon Web Services, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, CrowdStrike, Dassault, DocuSign, Dropbox, Graphisoft, IBM, Informatica, Intel, MathWorks, Microsoft, Nikon, Okta, Oracle, Prokon, PTC, Rockwell, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

Providing Clarity of Covered Operations and Information in a Transparent Manner (Chapter 3-6, Supplementary Provision / "ISMAP-LIU Cloud Service Registration Rules (Draft)")

ISMAP-LIU introduces a new pre-application process for cloud service providers (**CSPs**). In contrast to ISMAP, applications for ISMAP-LIU certification will be judged by the competent ministries prior to applying for service registration. This pre-application requires CSPs to attach the result of (an) impact assessment(s) conducted by user government agencies on the operations and information to be handled by the SaaS offered by the applicant.

The intention of this new mechanism is to provide an expanding list of representative examples of operations applicable for ISMAP-LIU registration. However, we are concerned that this approach may result in an overly narrow list of eligible services.

"The Guidance for Impact Assessment of Operations and Information for ISMAP-LIU" is designed to assist government agencies to determine whether the risk level of operations is low enough to warrant use of ISMAP-LIU. However, the ambiguity of the presented criteria makes it difficult for applicants and government agencies to assess the applicability to ISMAP-LIU in advance.

We recommend, instead of providing a List of Covered Operations, the relevant agencies should establish a list of more sensitive operations that require certification to the ISMAP system and indicating that operations not included on that list are eligible for ISMAP-LIU certification.

Implementing these recommendations will improve the predictability for CSPs regarding which services are eligible for ISMAP-LIU certification. This will encourage CSPs to offer the most cost-effective, secure, and high-quality services to the Government of Japan (**Government**).

Refining the Assessment Process (Chapter 5 Examination of Pre-Application, Chapter 7 Requirements to Applicant / "ISMAP-LIU Cloud Service Registration Rules (Draft)")

Reducing the number of controls subject to external audit is a helpful improvement over the current ISMAP requirements. However, the relevant agencies can further improve the assessment process and reduce the burden on limited government resources by implementing the following recommendations for both ISMAP-LIU and the current ISMAP:

- **Expediting the procedure for pre-application.** For the examination of pre-applications, 5.3 of draft ISMAP-LIU Cloud Service Registration Rules states that in the case the operation does not fall under the List of Covered Operations, "the determination of the applicability of the ISMAP-LIU for pre-application submitted during the first and second halves of each fiscal year shall be made, in principle, collectively by three months after the last day of each half year". Limiting review of the pre-applications to specified periods twice a year will lead to significant delays in cloud service adoption by procuring ministries and agencies. We urge expediting this process by setting the same examination period regardless of whether or not the operation is on the List of Covered Operations.

- **Reduce repetitive auditing process.** Exempting separate assessments of security controls already demonstrated through compliance with and certification to internationally recognized standards would streamline the auditing processes. Many CSPs are certified for internationally recognized standards (e.g., the ISMS-JISQ/ISO 27000 series) by internationally accredited certification bodies. Recognizing such certifications and eliminating duplicative local audits and other repetitive procedures and requirements to reuse evidence already provided during prior certifications will alleviate an unnecessary burden and delay for all stakeholders involved, including the Government. This will also encourage more companies in Japan to obtain ISMS/ISO certification, opening up greater international business opportunities for such Japanese companies, while also increasing competition to provide better and more cost-effective solutions to the Government.

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

- **Establish clear audit guidelines that are mapped to internationally recognized standards**. Discrepancies in the interpretation of security controls amongst ISMAP administrators, auditors, and CSPs imposes inefficiencies, additional costs, and delays. In some cases, CSPs that have undergone audits have experienced repeated requests from ISMAP administrators to re-audit because of differences in the interpretation of security controls by ISMAP administrators and auditors. We recommend establishing consistency in the interpretation amongst relevant stakeholders.

- **Enable Flexible Audit Period.** The current ISMAP and ISMAP-LIU stipulate fixed audit periods, to be selected upon the first registration. The audit cycle is then established going forward and flexibility is not afforded to adjust the audit cycle afterwards. This rigid audit cycle will not allow CSPs undergoing changes in their global audit cycles to adjust accordingly and may create a gap in the ISMAP assessment process which could result in temporary revocation of their services from the ISMAP and ISMAP-LIU Cloud Service List. To resolve this, we encourage the relevant agencies to adopt a system similar to the bridge letter of System and Organization Controls (SOC)[2] that covers the void between the most recent audit report's end date and the starting date of the next audit report. The bridge letter states that no material changes in the controls have taken place during the gap period and allows for the certification to be maintained during such circumstances.

  Also, under the current system, the submission of audit report is to be made within four months from the end of the audit. As this does not enable sufficient time for CSPs to collect all the required evidence, we recommend enabling a longer period of six months to make the system more implementable.

- **Establish a less frequent auditing schedule**. In contrast to the ISMAP's existing requirement to conduct audits on an annual basis, international cloud security best practices generally require audits once every three years. A less frequent audit schedule will reduce unnecessary costs to CSPs and the Government 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 diverting other important resources, and placing an increased burden on procuring agencies that will be required to renew the associated contracts yearly.

- **Accept ISMAP registration throughout the year**. Currently, the ISMAP administrators accept ISMAP registration on a quarterly basis, which may cause three-month delays or more for CSPs seeking ISMAP certification. Such delays can preclude companies from bidding for valuable procurement opportunities, denying the CSP the business opportunity and the procuring agencies the benefits of the cloud services in question.

[2] https://jicpa.or.jp/specialized_field/files/2-8-33-2-20200914.pdf
Q15: page 19-20

Continuous registration throughout the year will enable ISMAP to incorporate rapidly evolving cloud technology more quickly.

- **Increase the number of auditing firms registered under ISMAP.** We appreciate that relevant ministries recognize that the limited number of accepted auditing firms has resulted in a lack of resources to fulfill current and future demands for audit procedures required under ISMAP. We look forward to seeing increased number of registered auditing firms from the five currently registered, as this will alleviate bottlenecks and promote fair competition among auditing firms, providing CSPs with a wider variety of choice and potentially driving efficiencies in the auditing market.

  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.

Implementing the improvements to the ISMAP described above and reflecting them in ISMAP-LIU will lead to greater proliferation of security-assured cloud services in Japan, benefiting a wide range of stakeholders in both the public and private sectors.

Conclusion

BSA appreciates the opportunity to comment on the draft documents for ISMAP-LIU. In the future, we strongly urge relevant agencies to provide at least 30 days for comment to enable sufficient time for stakeholders to fully review multiple documents and discuss the proposed approaches. We hope that our recommendations will be useful in completing the documents. BSA looks forward to the opportunity to discuss how BSA and our members can work closely together with relevant agencies to implement the recommendations and expand options for government procurement, generating value for government investment in cloud services provided by the private sector.