BSA'S COMMENTS ON THE REPORT FROM THE COMMITTEE ON SECURITY ASSESSMENT OF CLOUD SERVICE (Draft)

December 25, 2019

BSA | The Software Alliance (**BSA**)[1] welcomes this opportunity to provide input to the Ministry of Internal Affairs and Communications (**MIC**) and the Ministry of Trade, Industry, and Economy (**METI**) on the draft Report from the Committee on Security Assessment of Cloud Service (**Report**).

Statement of Interest

BSA commends MIC and METI on their efforts to establish procedures for the proposed system for cloud service security assessment (**Assessment System**) with the goal of promoting cloud adoption across government agencies.

BSA members offer cutting-edge cloud computing technologies and services that help governments be more nimble, productive and innovative, while also improving network security and system availability. BSA and our members stand ready to contribute to the acceleration of government digitalization with security and would like to offer the comments below to support this goal.

Recommendations

We understand that this draft Report focuses on the roles and responsibilities of stakeholders and on documents and other details regarding the Assessment System process. We also understand that the release of the Assessment System standards and specific implementing rules will take place in 2020. We encourage MIC and METI to continue engaging stakeholders during the finalization and implementation of the Assessment Framework and prior to the release of the standards. We look forward to sharing, during this process, the expertise BSA members have developed through extensive work with governments around the world to improve operational efficiency using cloud computing and other software-enabled solutions.

We offer the preliminary recommendations below to contribute to your efforts.

Leveraging Internationally-Recognized Standards

As we addressed in our earlier submission in April,[2] it is important to recognize that cloud service providers (**CSPs**) often operate in multiple markets simultaneously, drawing upon geographic dispersion and economies of scale to provide more effective, reliable, and secure

[1] BSA (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. BSA's members include: Adobe, Akamai, Amazon Web Services, Apple, Autodesk, AVEVA, Bentley Systems, Box, Cadence, Cisco, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, Siemens PLM Software, Sitecore, Slack, Splunk, Symantec, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

[2] BSA's Comments on the Interim Summary from the Committee on Security Assessment of Cloud Service https://www.bsa.org/files/policy-filings/04162019bsasecurityassessmentcloudservice.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

software-enabled services. Therefore, it is critical that policies designed to promote the adoption of secure and effective cloud services must be ***globally interoperable*** with other public sector cloud security assessment and certification schemes and ***compatible with internationally-recognized standards***.

Section 2.2 of the Report articulates that the security controls in the Assessment System will use internationally-recognized standards as the base reference, but certain unique security controls will be added if the Government of Japan determines that such unique controls are indispensable for the satisfaction of Common Standards for Information Security Measures for Government Agencies and Related Agencies (**Common Standards**)[3] or are necessary procurement requirements. Thus, BSA's understanding is that the core component of the Assessment System's controls will be identical to those of internationally recognized standards.

If the Assessment System's core controls are not based upon those of internationally-recognized standards, companies, including Japanese companies, that follow internationally-recognized standards and undergo audits based on such standards will be confused by duplicative security controls in Japan. Also, given that the Assessment System is expected to be used as a reference by the private sector when assessing cloud security, duplicative requirements that are inconsistent with those of internationally-recognized standards could deter private sector cloud adoption in Japan as well, harming productivity, security, economic growth and job creation.

Therefore, we recommend limiting additional controls to only those that are carefully scrutinized, highly selected, and deemed indispensable controls of the Common Standards or NIST SP800-53. Such additional controls must maintain alignment with internationally-recognized standards.

Risk-Based, Outcomes-Oriented Requirements Instead of Prescriptive Requirements

While we recognize that the standards that will be used in the Security Assessment process need to encompass a range of security measures to ensure the protection of government information and systems, onerous, overly burdensome, and highly prescriptive requirements that do not contribute to enhancing cloud security would be counterproductive. Instead, such requirements would likely result in long and costly procedures that would demand upfront investment by CSPs, and, as discussed above, would deter the adoption of cloud technologies instead of accelerating its utilization in government agencies. Such requirements may also become a barrier for innovative CSPs to enter into Japanese market considering that the Assessment System might be used by the private sector as well.

Prioritization of essential controls is critical for driving effective outcomes. Such prioritizing in audits will enable CSPs to sensibly and appropriately select security measures for the cloud services which they seek to register. To streamline the Assessment System process, it is of paramount importance to **recognize existing certifications to internationally-recognized standards**. We strongly encourage that the Assessment System implement an expeditious audit and assessment process that leverages existing certifications. Specifically, the audit process should recognize existing certification reports and allow the reuse of evidence used in developing other reports.

Also, Sections 1.5. and 1.6 of the Report indicates that audits will be required every year for all security measures of registered cloud services. We recommend the Government of Japan to minimize unnecessary burdens on CSPs and consider a less frequent auditing schedule that focuses on priority security controls to make better use of limited resources.

Rather than focusing on new controls customized for the Government of Japan, the Assessment System should focus on outcomes as a better way to assess the controls designed

[3] Common Standards for Information Security Measures for Government Agencies and Related Agencies released by National center of Incident readiness and Strategy for Cybersecurity (NISC) at https://www.nisc.go.jp/eng/pdf/kijyun30-en.pdf

to deliver improved security. This would allow CSPs to continuously develop and deploy innovative technologies and information security solutions. Highly prescriptive and customized control-based standards do not guarantee improved security and can force CSPs to focus resources and effort on unique local controls rather than focusing on more meaningful security outcomes. BSA therefore urges the Government of Japan, when developing the Security Assessment standards and specific implementing rules, to **clearly define security objectives focused on outcomes, allowing CSPs to achieve these objectives through flexible mechanisms, instead of being required to comply with specific mechanisms for attaining those outcomes.** In this regard, ISO/IEC 27017, which consists of objectives/controls and Implementation guidance for cloud services will be a useful reference.

Security Not Related to Physical Location of Data Storage or Processing

Section 2.2(5) of the Report indicates that CSPs will be required to provide information, including the location of data centers, as part of the Assessment System process, although the Report notes that establishing a data center in Japan is not uniformly required for the Level 2 register. **We urge the Government of Japan to refrain from suggesting that data stored outside Japan will be less secure than data kept in the country.** We also ask government agencies to recognize that the focus should be on ensuring data is kept secure regardless of where it is stored. In this regard, the proposed focus on security objectives can offer the Government of Japan proof of appropriate security even when the data is stored outside of Japan.

It is important to recognize that data security is not dependent on the physical location of the data or the location of the infrastructure supporting it. Instead, security is a function of the quality and effectiveness of the mechanisms and controls maintained to protect the data. Companies consider many factors when deciding where to locate digital infrastructure such as servers and gateways, including maximizing Internet speed and access, implementing redundancy and backup capabilities, and ensuring the deployment of state-of-the-art security for user data.

Ensuring the Assessment System Applies Government-Wide

Considering that the goal of the Assessment System is to provide secure cloud services across all government agencies, it is also important that the Assessment System's rules are uniformly adopted and do not result in fragmentation between agencies, particularly in the classification of information systems based on "confidentiality", "integrity" and "availability". Providing clarification and unifying approaches, as well as encouraging collaboration among government agencies, will provide a less complex environment for all stakeholders involved in the Assessment System process.

The services of government agencies vary widely, making it difficult for the Assessment System to cover all security controls for all services of government agencies. In the cloud computing environment, security controls of services are generally covered in individual Cloud Service Level Agreement (Cloud SLA). Our understanding, based on the report, is that the Assessment System covers the core, fundamental security controls, and other extended security controls will be agreed between the procurer and CSP under the Cloud SLA upon the procurement of government service under this Assessment System. We recommend that this point be clarified for stakeholders involved in the Assessment System.

Organizing Structure and Ensuring Effectiveness to Use Systems in the Government

In addition, we note that some types of information that CSPs may be required to share with auditors and government agencies may be proprietary and, therefore, should be subject to non-disclosure agreements. In addition, it is very important to carefully consider the appropriate scope of information to be publicized in the register.

With the full launch of the Assessment System set to start by fall of 2020, we also encourage the Government of Japan to provide visibility on concrete plans to drive adoption across government agencies. The implementation of the Assessment System will need to be coupled

with efforts to raise awareness amongst agencies to achieve the intended goal of realizing Japan's transformation to digital government.

Conclusion

BSA appreciates the opportunity to submit comments on the Report and we look forward to continuing supporting MIC and METI's efforts to increase secure cloud adoption by government agencies in Japan. We stand ready to answer any questions you may have and to discussing this further.