# BSA'S COMMENTS ON THE INTERIM SUMMARY FROM THE COMMITTEE ON SECURITY ASSESSMENT OF CLOUD SERVICE

## April 16, 2019

### Statement of BSA Interest

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 Interim Summary from the Committee on Security Assessment of Cloud Service (**Interim Summary**).

BSA commends the commitment of MIC and METI to increase cloud adoption across the government and improve procedures for security assessment of cloud services. We are encouraged to see that the Interim Summary recognizes the importance of the "Basic Policy on Use of Cloud Services in Government Information Systems" compiled by the Liaison Conference of CIOs,[2] which promotes the 'Cloud-by-Default Principle'. We also welcome that the Government of Japan has reviewed various cloud adoption practices in countries outside of Japan to inform the drafting of the Interim Summary.

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.

Cloud services providers (**CSPs**) often operate in multiple markets simultaneously, drawing upon geographic dispersion and economies of scale to provide more effective, reliable, and secure software-enabled services that even the most heavily resourced firms cannot provide on their own. 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***.

Moreover, when considering mechanisms to assess cloud security for the use in the public sector, such mechanisms must recognize that there are different cloud computing service models, ranging from Infrastructure-as-a-Service (**IaaS**) and Platform-as-a-Service (**PaaS**) to Software-as-a-Service (**SaaS**). These models differ from one another in various ways, including

---

[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, 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, Slack, Splunk, Symantec, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

[2] Basic Policy on Use of Cloud Services in Government Information Systems found at https://cio.go.jp/sites/default/files/uploads/documents/cloud_%20policy.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

in the relationship between the CSP and its users and customers and the nature of allocating shared responsibility for security, operational efficiency, and reliability in the cloud environment and as such, there should not be a one-size-fits-all approach. This shared responsibility is frequently described in the Cloud Service Level Agreement (Cloud SLA).

Furthermore, the proposed system to assess security of cloud services (**Assessment System**) needs to ensure that risk-based approaches and multi-layered defense systems following a "defense-in-depth" approach will be adopted uniformly across government agencies so that it will promote the adoption of secure and effective cloud services by government agencies and others who may follow the assessments in the future.

## Recommendations

Beyond these overarching policies, BSA offers specific comments on certain sections of the Interim Summary below:

### Section 2: Classification of Information Systems and Section 4.4: Architecture of Overall System

The Interim Summary's guidance on classification of information and information systems provides important considerations for approaching security in cloud computing systems. As cloud services have evolved, innovations in cloud architectures have enabled the application of security rules according to different security, privacy, and functionality needs within a given cloud architecture, such as by using separate containers applying different sets of controls. These innovations have improved the flexibility and diversity of possible solutions to meeting security needs in cloud systems.

Cloud security policies should recognize these innovations and accommodate the flexibility and diversity of different approaches to ensuring security of sensitive information. Sections 2 (Classification of Information Systems) and 4.4 (Architecture of Overall System) of the Interim Summary recommend that "separation of systems" should be considered as a methodology to protect sensitive information. However, it should be recognized that physical separation of information systems from each other, in the context of advanced cloud computing architectures, is often unnecessary from a security standpoint, and may have unintended consequences, such as reducing access and utilization of information stored in such systems, as well as creating a false sense of security.

Also, we continue to have concerns regarding the suggestion in the Common Standard for Information Security Measures for Government Agencies (FY 2018) that physical network separation is an information security solution when instead, physical network separation may increase cybersecurity risks by interfering with the benefits of real-time security updates (see Sections 5.2.1-(2)a of the Common Standards). Please refer to BSA's submission[3] when reflecting the cloud security assessment discussion in the Common Standards. Cloud security policies should promote a multi-layered approach to cybersecurity defenses, with specific controls and computing environments tailored according to the security, privacy, and functionality needs of users.

In addition, approaches to classifying information should be aligned with existing best practices. In particular, we recommend using the US National Institute for Standards and Technology's Special Publication 800-60[4] and its Federal Information Processing Standard (FIPS) 199[5] as guides for categorizing sensitive information.

---

[3] See BSA Comments on the GOJ Common Standards for Information Security Measures for Government Agencies (FY 2018) – June 28, 2018 at:
https://www.bsa.org/~/media/Files/Policy/Data/06282018BSACommentsGOJ2018CommonStands_en.pdf
Japanese translation at:
https://www.bsa.org/~/media/Files/Policy/Data/06282018BSACommentsGOJ2018CommonStands_jp.pdf

[4] SP 800-60 Vol. 1 Rev. 1: Guide for Mapping Types of Information and Information Systems to Security Categories, at:
https://csrc.nist.gov/publications/detail/sp/800-60/vol-1-rev-1/final

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

## Section 3.2: System Framework

BSA fully supports the proposal that the framework should enable maximum utilization of existing mechanisms and certification systems. In this regard, we encourage the Government of Japan to ensure the Assessment System will implement a sufficiently expeditious audit and assessment process.

The Interim Summary states it is necessary to design the Assessment System so that, in terms of the overall system procurement, costs can be reduced compared to costs before implementing cloud services in order to leverage the advantage of implementing cloud services. This is an important point, and when comparing the total cost of implementing cloud computing solutions to conventional information systems, not only must the procurement costs be included, but also other costs, such as personnel, maintenance, physical security of premises, etc. In other words, it is very important to compare the total costs operation between on-premises and cloud computing services. Having said that, it is also important to recognize that cost is not the only factor in deciding whether to use cloud services. Flexibility should exist to allow procurement criteria to also include other factors such as the performance, latency and other potential trade-offs to ensure that the solution ultimately meets the user requirements.

## Section 3.3: Detailed Design of System

Private Sector Participation in Standards Development:

The draft management standards which will be developed by around summer 2019 are very important and critical to CSPs. We encourage the Government of Japan to be transparent during this development process for the management standards and their related policies, guidelines, and rules, and to consult with affected stakeholders, including BSA members, throughout the process. Before the Government of Japan makes critical decisions, soliciting feedback from CSPs is essential to ensure the relevant standards and policies are adequately informed by private sector expertise.

Risk-Based, Outcomes-Oriented Requirements Better than Prescriptive Requirements:

The Assessment System and its related rules should allow government agencies to adopt open systems and control information according to their respective confidentiality classification, etc., using encryption, authentication, and other functionalities provided by CSPs.

Regarding the management standards, an outcome focused approach is critical, as this better allows CSPs to continuously innovate and develop new technology and information security solutions better than when such standards are highly detailed. Prescriptive security controls quickly become obsolete and stifle a government's ability to take advantage of the latest security breakthroughs. The management standards should therefore set out clearly defined objectives, focused on outcomes, instead of prescribing specific mechanisms for attaining those outcomes.

Security Not Related to Physical Location of Data Storage or Processing:

The Interim Summary suggests creating standards for physical aspects, such as standards for data centers which operate cloud services. In this regard, optimizing and ensuring smooth cross-border data transfers on a global scale are vital to maximizing the benefits of cloud-

[5] FIPS PUB 199: Federal Information Processing Standards Publication: Standards for Security Categorization of Federal Information and Information Systems, at: https://csrc.nist.gov/csrc/media/publications/fips/199/final/documents/fips-pub-199-final.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

computing services, including economies of scale and cost benefits, redundancy for back-up systems, and real-time updates of systems in response to global cybersecurity threats.

### Section 4.5: Organizing Structure and Ensuring Effectiveness to Use Systems in the Government

Some information shared between auditors, government agencies as cloud service customers or users, and CSPs may be confidential information belonging to the CSPs and therefore subject to non-disclosure agreements between the relevant parties. In this regard, it is very important to carefully consider the appropriate scope of information to be publicized in the register.

We also urge MIC and METI to ensure an appropriate transitional process by which government agencies may use or continue to use cloud services even during the development phase of the register when many cloud service providers are not yet registered.

## Conclusion

BSA appreciates the opportunity to submit our comments on the Interim Summary. We hope this will be useful in finalizing the Interim Summary. BSA welcomes opportunities to collaborate with MIC and METI on developing the Assessment System and we sincerely hope that our member companies and other CSPs may contribute to creating the management standards and their related rules and participate in the simulations envisioned in Section 4.1. Please let us know if you have any questions or would like to discuss these comments in more detail.

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