February 26, 2024

BSA COMMENTS ON PROPOSED AMENDMENTS TO THE CLOUD SECURITY ASSURANCE PROGRAM

Submitted Electronically to the Ministry of Science and ICT

BSA | The Software Alliance (**BSA**)[1] welcomes the opportunity to provide comments to the Ministry of Science and ICT (**MSIT**) regarding the proposed amendments to Korea's Cloud Security Assurance Program (**CSAP**), which outline cloud security certification requirements for data systems classified under the "Medium" and "High" grades.

BSA is the leading advocate for the global software industry before governments and in the international marketplace. BSA members create the technology products and services that power other businesses, including cloud storage services, customer relationship management software, human resources management programs, identity management services, security solutions, and collaboration software. Our members have made significant investments in Korea, and we are proud that many Korean entities and consumers continue to rely on our members' products and services to do business and support Korea's economy.

Summary of BSA's Recommendations

1. Allow more public institution data systems to be classified under the "Low" grade and remove references to personal information in the CSAP, given that Korea's Personal Information Protection Act (**PIPA**) already stipulates safeguards for protecting personal information held by public institutions. This would allow substantially more public institutions to use the cutting-edge cloud services provided by global cloud service providers (**CSPs**).

2. Adjust requirements for CSPs to obtain certification for "Low" and "Medium" grades. In particular, for "Low" and "Medium" grades, which will constitute most of the data handled by public institutions, requirements for physical network separation, data residency, use of Korea-developed encryption algorithms and local personnel presence should not apply. The CSAP should also accept internationally recognized standards and certifications from internationally accredited bodies.

Overview of CSAP and its amendments

In January 2023, MSIT amended the CSAP to create a tiered system. Pursuant to the *Public Notice on Cloud Security Assurance Program* (**Public Notice**), the systems of administrative agencies and public institutions (collectively, **public institutions**) were classified into three grades — "High",

[1] BSA's members include: Adobe, Alteryx, Altium, Amazon Web Services, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, Cloudflare, CNC/Mastercam, Dassault, Databricks, DocuSign, Dropbox, Elastic, Graphisoft, Hubspot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Nikon, Okta, Oracle, PagerDuty, Palo Alto Networks, Prokon, Rockwell, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Workday, Zendesk, and Zoom Video Communications, Inc.

300 Beach Road
#30-06 The Concourse
Singapore 199555

P: +65 6292 2072
F: +65 6292 6369
W: bsa.org

Regional Representative Office
UEN: S97RF0005K

"Medium", and "Low" — depending on the sensitivity of data handled. The Public Notice also established requirements for managing data systems at the "Low" grade.

CSPs certified to manage public institution data systems at the "Low" grade: a) may manage a public institution's data if the data system is open, public, and does not contain personal information; and b) are not required to use physical network separation and instead may use logical network separation to keep customer workloads distinct. However, even under "Low", CSPs need to ensure data residency and use only Korea-developed encryption algorithms (i.e., ARIA and SEED) rather than those more widely used and vetted internationally. In addition, the "operational personnel" for cloud computing services used by public institutions needed to be "limited to Korea".

Unfortunately, despite these changes to the CSAP, no foreign CSP has managed to obtain CSAP certification for the "Low" grade systems thus far. This will be further compounded by the recently proposed amendments to the Public Notice, which not only did not relax requirements for the "Low" grade but would make "Medium" and "High" grades significantly more difficult to get certified for, especially for foreign cloud service providers. In this regard, BSA notes that:

- There are proposed amendments to existing requirements for all grades, including "Low". Notably, "management consoles" are now also need to be separated from the "cloud computing service area" used by general users.
- Additional requirements for "High" will be introduced, which include "external network blocking, integrated management of security audit logs, account and access rights automation, and security automation items". These additional requirements go beyond the already strict requirements that were in place before the CSAP was amended in 2023.

The proposed amendments run counter to the Government's efforts to promote adoption of cloud solutions within the public sector, and disincentivizes IT vendors from developing and providing more efficient security solutions. As such, we urge MSIT to make further amendments to the CSAP framework, as set out below.

Allow more public institution data systems to be classified under "Low"

The Public Notice continues to specify that a public institution's data system would be classified as "Low" if it is an open, public data system that does not contain any personal information. This is a narrow classification that captures only a small subset of public institutions. Specifically, if a public institution's data system contains personal information, which is broadly defined in Korea's PIPA,[2] it would be classified as either "Medium" or "High". This would result in the *majority* of public institution data systems requiring CSPs to correspondingly obtain a CSAP certification for "Medium" or "High" grades to provide their services to the Korea public sector.

Consequently, despite the removal of physical network separation requirements for the "Low" grade, the CSAP continues to prevent majority of public institutions from using services provided by global CSPs, even when those services provide wider functionality, competitive pricing, and strong security. Many global CSPs invest enormous resources in their cybersecurity capabilities and constantly evaluate and upgrade their security processes and systems to deal with the latest cyber threats from around the world. As the capabilities of malicious actors in cyberspace evolve, governments need to ensure that they have the best tools at their disposal to deal with emerging cyber threats emerging from anywhere in the world. If global CSPs that have developed effective cybersecurity solutions are limited to providing services to a small pool of public institutions that do not deal with personal

[2] Article 2 of the PIPA defines "personal information" as any of the following information relating to a living individual:
a) information that identifies a particular individual by his or her full name, resident registration number, image, etc.;
b) information which, even if it by itself does not identify a particular individual, may be easily combined with other information to identify a particular individual. In such cases, whether or not there is ease of combination shall be determined by reasonably considering the time, cost, technology, etc. used to identify the individual such as likelihood that the other information can be procured; and
c) information under items (a) or (b) above that is pseudonymized in accordance with subparagraph 1-2 below and thereby becomes incapable of identifying a particular individual without the use or combination of information for restoration to the original state (hereinafter referred to as "pseudonymized information").

information, a Korean public institution dealing with personal information would, counter-intuitively, be unable to avail itself of cutting-edge cybersecurity options provided by global CSPs, which may be better suited for their needs.

Moreover, personal information held by public institutions are already subject to a range of privacy-focused safeguards under the PIPA. The PIPA limits how personal information controllers – which include public institutions – may collect, use, and disclose personal information. In doing so, the PIPA also recognizes that personal information includes a wide variety of data types, which may raise different grades of sensitives. For example, it applies many safeguards to all personal information, but imposes additional limits on the processing of certain "sensitive information."[3] In addition, the PIPA requires personal information controllers, including public institutions, to take technical, managerial, and physical measures to preserve access to personal information and to protect it against loss, theft, and other damage.[4] Given these existing safeguards, it is unnecessary to introduce further obligations by classifying data containing personal information as "Medium" or "High".

BSA recommends allowing more data systems to be classified under the "Low" grade. In this regard, the Government should remove references to personal information in the CSAP, given that the PIPA already stipulates safeguards for protecting personal information held by public institutions. This would allow substantially more public institutions to use the cutting-edge cloud services provided by global CSPs.

Adjust requirements for "Low" and "Medium" Grades

CSAP certification for all three grades will continue to require data residency, use of Korea-developed encryption algorithms and local personnel presence. In addition, for "Medium" and "High" grades, CSPs are still required to physically separate their networks. The "High" grade is also required to take on even more obligations beyond current CSAP requirements, which include "external network blocking, integrated management of security audit logs, account and access rights automation, and security automation items".

BSA appreciates that it is crucial to ensure that adequate protections are in place for "High" grade systems, which cover the most sensitive categories of information, including those relating to national security. However, many of these requirements for "High" also apply to "Low" and "Medium" grades. These requirements impose excessive technical and administrative burdens that do not enhance security but act as barriers to many global CSPs:

- **Physical Network Separation:** Except for the proposed "Low" grade, CSAP requires CSPs to physically separate the networks providing services to public sector institutions. While a few countries retain physical separation requirements for highly sensitive data (e.g., data related to national security and defense), it is rarely applied throughout the public sector, including for workloads or institutions that handle less sensitive (and sometimes, public) data. The uniformly applied physical network separation requirement in the CSAP does little to enhance security while undermining the main benefit of cloud computing services, which is the economy of scale and state-of-the-art security capabilities of multi-tenant cloud services.

- **Encryption:** CSAP prohibits CSPs from using other generally accepted, internationally recognized encryption algorithms when offering cloud services to public institutions. This is impractical for many CSPs that already use state-of-the-art encryption algorithms that meet internationally recognized standards and are accepted for applications in the most sensitive circumstances in other markets.

- **Data residency:** CSAP requires CSPs to ensure all public sector data must be physically located in Korea. This is an unnecessary barrier for many CSPs that store, process, and

[3] See PIPA Art. 23 (Limitation to Processing of Sensitive Information).

[4] See PIPA Art. 29 (Duty of Safeguards).

backup data in regional data centers outside of Korea. The use of offshore data centers to ensure redundancy and backup is a mechanism to enhance data security; in case of a serious cyberattack or physical disruption, including natural disasters, data stored in physically remote data centers can be used to recover from the incident.

- **Local Personnel Presence:** CSAP requires the operations and management personnel of cloud service providers to be located within the territory of Korea. Such local presence obligations discriminate against foreign companies. More importantly, they substantially undermine the scalability advantages offered by cloud computing, as CSPs will be required to duplicate their management and operations personnel separately at each of their overseas operational sites, substantially complicating company operations and increasing compliance costs.

Beyond preventing the majority of public institutions from using services provided by global CSPs with high quality security capabilities, as highlighted above, these CSAP requirements will drive up costs for CSPs and Software-as-a-Service (SaaS) providers without tangible security benefits, frequently weakening the cybersecurity of Korean public sector institutions. For example:

- Instead of recognizing certifications that are carried out by external accredited assessors and based on internationally recognized standards, CSAP requires additional and duplicative local verification of existing certifications, which increases costs to CSPs and slows cloud adoption.

- Data residency/localization requirements prevent CSPs from using off-shore data centers to ensure redundancy and data backup. They also distort the market for cybersecurity solutions by placing undue value on which companies are best at complying with data localization requirements rather than which companies are best at providing the best functioning and most secure solutions.

- Requiring CSPs to use Korea-developed encryption algorithms (e.g., ARIA, SEED) as opposed to widely-adopted and state-of-the-art encryption algorithms leads to increased fragmentation of the global cybersecurity landscape. This drives up compliance costs while also depriving public sector institutions from using best-in-class encryption technologies and creates interoperability challenges between systems using widely used and vetted encryption algorithms that meet internationally recognized standards.

- Many Korean-based SaaS providers also rely heavily on the cloud infrastructure provided by global CSPs in offering their services in Korea and other markets.[5] Due to CSAP, these domestic SaaS providers may not be able to provide their services to public institutions in Korea. The loss of opportunities for domestic SaaS providers will also further limit the growth and development of Korea's domestic cloud service industry.

We therefore urge the Government to take this opportunity to adjust requirements under the "Low" and "Medium" grades. In particular, for "Low" and "Medium" grades, which will constitute most of the data handled by public institutions, requirements for physical network separation, data residency, use of Korea-developed encryption algorithms and local personnel presence should not apply. In addition, the CSAP should also accept internationally recognized standards and certifications from internationally accredited bodies as demonstration that a CSP has implemented appropriate

[5] See "A collection of AWS top customer stories to watch in 2023", January 2023, https://aws.amazon.com/ko/blogs/korea/2022-customer-cases/. For example, STC Lab, which develops online traffic regulating solution called NetFUNNEL, was built on a suite of AWS cloud infrastructure services. STC Lab partners with Korean government agencies, such as the Ministry of Trade, Industry and Energy, as well as the Center for Disease Control. NetFUNNEL has been deployed for COVID-19 pre-reservation services and online elections.

security controls, and should consider recognizing certifications accepted by like-minded allies as demonstration of a vendor's security practices.[6]

Conclusion

To keep pace with ever evolving cyber threats, the Government of Korea needs to ensure that its public institutions can select from the best tools at their disposal, offered by a greater variety of domestic and global CSPs, to maximize the social and economic benefits of cloud technologies. Security concerns should be addressed by carefully calibrated solutions aligned with risk-based and internationally recognized standards, rather than restrictive, compliance oriented approaches, so that efforts to promote security do not come at the unnecessary expense of positive economic outcomes and counterproductive reductions in actual cybersecurity.

We thank MSIT for the opportunity to provide recommendations on the proposed partial amendments to CSAP. Please do not hesitate to contact BSA if you have any questions regarding this submission or if we can be of further assistance.

Sincerely,

Tham Shen Hong

Senior Manager, Policy – APAC

[6] Internationally recognized standards leverage global security expertise from governments, industry, and academia. For example, ISO 27001, "specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of an organization," while ISO 27017 provides "guidelines for information security controls applicable to the provision and use of cloud services."