REVISED KOREAN CLOUD SERVICES SECURITY ASSURANCE PROGRAM
Comments from BSA | The Software Alliance
August 8, 2019

BSA | The Software Alliance (**BSA**)[1] welcomes this opportunity to provide comments on the intended revisions to Korea's Cloud Security Assurance Program[2] (**Program**) announced by the Ministry of the Interior and Safety (**MOIS**) and Ministry of Science and ICT (**MSIT**) on July 23, 2019[3].

Statement of Interest

BSA's members are at the forefront of data-driven innovation, including cutting-edge advancements in data analytics, machine learning, and the Internet of Things, among others. To ensure consumers and businesses alike can trust in and reap the maximum benefits from these innovations, our members remain deeply committed to maintaining a high quality of service across their platforms and services.

BSA's members further earn users' confidence by providing essential security technologies, including encryption, to protect customers from cyber threats. These threats are posed by a broad range of malicious actors, including those who would steal citizens' identities, harm their loved ones, steal commercially valuable secrets, or pose immediate danger to national security.

BSA and our members thus have a significant interest in the Program, in particular the certification requirements under the Program, and would like to offer the following comments and recommendations on how these can be further improved.

General Comments

BSA commends MOIS's and MSIT's objective of promoting the use by government agencies of Software-as-a-Service (**SaaS**) cloud services, by simplifying the certification requirements for SaaS services under the Program, thereby reducing the burdens for SaaS service providers. This approach to having the public sector increasingly leverage the power and benefits of cloud services gives strong

[1] BSA (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. BSA's members are at the forefront of data-driven innovation, including cutting-edge advancements in data analytics, machine learning, and the Internet of Things. They earn users' confidence by providing essential security technologies, such as encryption, to protect customers from cyber threats.

BSA's members include: Adobe, Akamai, Amazon Web Services, Apple, Autodesk, AVEVA, Baseplan Software, Bentley Systems, Box, Cadence, Cisco, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens PLM Software, Sitecore, Slack, Splunk, Symantec, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

[2] The current Program is currently accessible at: https://isms.kisa.or.kr/main/csap/intro/index.jsp

[3] As announced at: https://www.msit.go.kr/web/msipContents/contentsView.do?cateId=mssw311&artId=2093939

effect to Korea's Cloud Promotion Act[4]. It is also well-aligned with the 'cloud-first' policies that governments around the world are adopting[5].

To fully realize MOIS's and MSIT's objective, the Program could be further improved by adopting additional revisions to the certification requirements. In particular, BSA would like to request that MOIS and MSIT consider deleting the following items:

- **14.2.1 (Physical location and separation)** which requires that "*the physical location of the cloud system and data shall be restricted to in county and cloud service area for public institutions shall be physically separated from the cloud service area for private institutions*"; and

- **14.3.1 (Provision of certified encryption technology)** which requires that "*cloud computing services providers shall use government-certified standard encryption technology when providing an encryption method for important material created through the cloud service*".

Our detailed comments on these two items are below.

Item 14.2.1 (Physical location and separation)

The introduction of any data/server localization or system separation requirements would have a negative impact on Korea's digital ecosystem and curtail its ability to participate effectively in the global digital economy. Such requirements raise the cost of providing services, as service providers will need to put in place duplicative and potentially under-utilized servers and other related infrastructure to allow for data to be localized and/or for networks to be physically separated. The costs associated with such additional infrastructure will need to be recovered, which would ultimately increase the costs for end consumers.

Data/server localization and network separation requirements would also inhibit the choice of technology available to end-users and procuring entities, including government agencies. Even if a service provider has hosting facilities in Korea, it is likely that some features or functionality of its services will be inhibited. In many cases, it will not be possible to process all data locally and yet provide the same quality of service as could otherwise be achieved – for example, with respect to certain fraud detection services that rely on the analytical power of commercial hyperscale cloud computing services.

To the extent that data security is the driving concern behind having data/server localization and network separation requirements (instead of permitting use of commercial hyperscale cloud services), these may be unfounded. Well-managed cloud services are often more secure than their on-premises counterparts. Because the cloud is their business, cloud service providers make significant investments to ensure their systems are secure, both physically and digitally. They typically go through stringent auditing processes to meet international security certifications, and are able to provide advanced threat protection technologies and secure data at rest and in transit. Cloud service providers operating globally also have visibility into cyber threats around the world, and ensure their cyber defenses are quickly updated against newly discovered threats. All these security advantages will be lost where organizations are required to localize their data/servers and physically separate their networks. In fact, this will potentially reduce the security and resiliency of systems used by such

[4] *Act on the Development of Cloud Computing and Protection of its Users*, Act No. 13234, Mar. 27, 2015.

[5] Including in Australia, New Zealand, the Philippines, and the United States of America.

organisations – bad actors will have a 'honeypot' to target, and it will be more difficult to identify and address threat vectors as those organizations will be unable to access advanced threat protection technologies.

At a broader level, by effectively restricting access to technologies that rely on the ability to transfer data across borders and that leverage commercial hyperscale cloud computing services, data/server localization and network separation policies will also negatively affect the use and development of new and innovative technologies within Korea, including AI and other emerging technologies, ultimately negatively affecting Korea's economic competitiveness in the global digital economy.

BSA would accordingly like to request that MOIS and MSIT consider deleting item 14.2.1.

14.3.1 (Provision of certified encryption technology)

As MOIS and MSIT are likely aware, encryption is a critical tool for protecting sensitive data, including personally identifiable information that can be used for identity theft, financial data exploited for fraud and other financial crimes, proprietary business information and intellectual property, and even government secrets. Although strong encryption cannot prevent a data breach, it can block cyber attackers from accessing the sensitive data once its stolen, thus mitigating the risk.

National approaches to encryption, however, have limitations because of the global nature of the Internet, and the fact that criminal or terrorist acts are not limited by national borders. In fact, fragmented and piecemeal approaches by individual countries towards only allowing the use of domestically-certified encryption standards may deprive organizations from using best-in-class encryption technologies, and this would weaken rather than strengthen the protection of sensitive data.

Accordingly, instead of imposing a requirement that only domestically-certified encryption technologies may be used, **BSA would like to request that MOIST consider deleting item 14.3.1. In its place, we would like to further request that MOIS and MSIT consider adopting a principled approach towards ensuring the security of information through the use of encryption**. In this regard, BSA has developed eight principles that MOIS and MSIT could consider implementing with respect to its policy on the use of encryption[6]:

1. **Improving data security**: Providers of data services — storing, managing or transmitting personal or business data — must be permitted to use the best available technology to thwart attacks against that data or the entities and individuals who depend on those services.
2. **Enhancing law enforcement and counter-terrorism capabilities**: Law enforcement agencies, subject to appropriate privacy and civil liberties safeguards, should have access to the best available resources, information, and tools available to prevent and prosecute terrorist and criminal acts.
3. **Promoting privacy**: Individuals have a right to be secure in their public, private and commercial lives and interactions.
4. **Protecting confidential government information**: National, state and local agencies should ensure that the data they hold is secure against threats of domestic and foreign intrusion.
5. **Encouraging innovation**: Developers and providers of innovative data security tools should be free of government mandates on how to design technology products and tools for digital security.

[6] For these and other resources developed by BSA on encryption, please visit https://encryption.bsa.org.

6. **Defending critical infrastructure**: Providers of essential services, such as banking, health, electricity, water and other critical infrastructure providers, should be empowered to provide the best available security technologies to their users. Best practices should be widely shared.
7. **Understanding the global impact**: Criminal and terrorist acts are not limited by national borders, and laws and policies must create consistency and clarity in all countries where security technologies are developed and used.
8. **Increasing transparency**: There should be full, transparent, and considered public dialogue before any legislative proposal concerning the future of technology mandates or encryption is adopted.

Conclusion

BSA has worked closely with governments around the world in relation to the development of consumer protection, data protection, and cybersecurity and encryption policies and legislation. In doing so, we have witnessed first-hand the potential for such policies and legislation to effectively encourage innovation whilst still protecting the interests and rights of consumers.

BSA would welcome an opportunity to meet and work with MOIS and MSIT on the refinement of the Program to ensure that it can meet MOIS's and MSIT's objectives, and we will be in touch with your respective offices to explore meeting arrangements.

BSA | THE SOFTWARE ALLIANCE