Ref	[Form] Proposal for Regulatory Improvement

Title	**Deregulating the Cloud Security Assurance Program (CSAP)**		
Authority Ministry	**Ministry of Science and ICT, Ministry of Interior and Safety**		
Proposer (entity, title Name)	Business Software Alliance, Korea Country Manager, Geun Kim	**Contact info.**	+82 10 9137 5100 Geun@bsa.org

□ **Content**

o **(Regulation)** Under the Cloud Act and relevant guidelines by the Ministry of Interior and Safety (**MOIS**), public institutions and administrative agencies (collectively, **"public institutions"**) may only adopt cloud services offered by cloud service providers (**CSPs**) that are certified under the Cloud Security Assurance Program (**CSAP**). Under the CSAP, CSPs are evaluated and certified based on compliance with the Ministry of Science and ICT's (**MSIT**) Information Protection Standards for Cloud Computing Services.

~~o~~ **(Problem/Dispute)** The CSAP imposes onerous technical and administrative burdens that do not enhance security but act as barrier to global CSPs. As a result, no global CSP has obtained CSAP. Examples of excessive requirements that are not in line with global standards include:

a) Physical Network Separation: Physical network separation is required throughout the public sector, without exception. While a few countries retain physical or logical network separation requirements for some highly sensitive areas (national security, defense), it is rarely applied throughout the public sector, including in workloads or institutions that handle non-sensitive (and sometimes, public) data, such as public universities and internal communications. The uniformly applied physical network separation 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.

b) Encryption: CSPs must use a government-permitted encryption algorithm (e.g., ARIA, SEED) to provide cloud services to public institutions. This is impractical for many leading 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.

c) Data residency: The cloud management system and its data must be physically located in Korea. This is an unnecessary barrier for many CSPs that store/process data in regional data centers outside of Korea. In some cases, the use of off-shore data centers is to ensure redundancy and back-up; in case of a serious physical or cyberattack on one data center, data stored in a physically remote data center can be used to recover from the incident.

The consequences are as follows:

o Public institutions in Korea are unable to use cutting-edge services provided by global CSPs. Due to various requirements such as data residency and network separation, the CSAP currently prevents public institutions from using services provided by global CSPs, even when those services provide better functionality, competitive pricing, and strong security. Many global CSPs invest enormous resources in their cybersecurity capabilities and constantly upgrade the security programs and controls on their cloud systems to deal with the latest cyber threats. 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. If companies that have developed effective cybersecurity solutions are not able to obtain CSAP certification given the constraints outlined above and are as such eliminated from the marketplace, a Korean public institution will have both more limited and more costly options that cannot provide cutting-edge cybersecurity.

o Loss of Opportunities for domestic Software as a Service (**SaaS**) providers. Many domestic SaaS providers rely heavily on the cloud infrastructure provided by global CSPs in offering their services. Due to CSAP, these domestic SaaS providers s are also unable 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.

o Increased costs and decreased security. CSAP requirements will drive up costs for CSPs and SaaS providers without tangible security benefits, and in some cases, even weakening security. For example:

a) 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.

b) Data residency/localization requirements prevent CSPs from using off-shore data centers to ensure redundancy and back-up of important data. 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.

c) Requiring CSPs to use a domestic/government-permitted encryption algorithm (e.g., ARIA, SEED), as opposed to widely-adopted and state-of-the-art encryption algorithms, will lead to increased fragmentation of the global cybersecurity landscape. This will drive up compliance costs while also depriving organizations from using best-in-class encryption technologies and create interoperability challenges between systems using other internationally recognized standards. This limitation will prove particularly problematic as the government transitions to a world with quantum computers.

※ (Oversea Examples) **US – FedRAMP**

The Federal Risk and Authorization Management Program (**FedRAMP**) was established to provide a cost-effective, risk-based approach for the adoption and use of cloud services by the US federal government. FedRAMP empowers agencies to use modern cloud technologies, with an emphasis on security and protection of federal information.

FedRAMP categorizes Cloud Service Offering (**CSO**) into one of three impact levels: low, moderate, and high. The impact levels are based across three security objectives: confidentiality, integrity, and availability following the Federal Information Processing Standard (**FIPS**) 199 standards.

Notably, FedRAMP only requires data localization for high-impact systems – agencies are then permitted to require data to stored in specific locations by contract. However, even the "high" impact level, physical network separation is not required, reflecting the US' view that physical network separation does not necessarily lead to more secure systems.

For moderate-impact and low-impact systems, the US Government's approach is similar to that of a private company: consider the data and its potential impact on the enterprise and make a risk-based decision about whether the enterprise is better served by simplicity, localization, or the implementation of compensating security controls. As a result of the risk-based approach, US government entities have a wide spectrum of cloud services to choose from, with six non-U.S. companies qualifying for FedRAMP, including some at the High assurance level.

o **(Suggestion) Reform CSAP by segmenting the public sector according to impact and security needs and adjust CSAP requirements based on each security classification of various public sector entities.**

a) BSA recommends that MOIS and MSIT adopt a similar approach to FedRAMP and implement different security classifications in the CSAP, taking into account the various public institutions' functions and the sensitivity of the data they deal with. This risk-based approach will give public institutions the flexibility to procure the cloud services that best fit their security needs, thus promoting the adoption of cloud within the public sector. This would also incentivize vendors to develop more effective and efficient security solutions.

b) In this regard, the Government should remove the physical network separation requirement (14.2.1), particularly for less sensitive entities, as it does little to boost security and diminishes security and resilience benefits provided by the commercial cloud, as well as the domestic/government-permitted encryption algorithm requirement (14.3.1) which deprives public sector organizations from using best-in-class encryption technologies that allow a transition to quantum computing.

c) CSAP should also allow the procurement of software developed and maintained in conformance with internationally recognized standards (e.g., ISO 9000 and 27000 series) or industry best practices, including the BSA Framework for Secure Software and the National Institute of Standards and Technologies (**NIST**) Secure Software Development Framework.

Related Law	Act on the Development of Cloud Computing and Protection of its Users Electronic Government Act
Type of Proposal	**■ New Proposal □ Re-Proposal**

E.O.D.