U.S. Chamber of Commerce

U.S.-Korea Business Council

February 9, 2023

Mr. Lee Jong-ho
Minister
Ministry of Science and ICT
194, Gareum-ro
Sejong-si, 30121, Republic of Korea

Mr. Heo Jin-woo
Director of Cyber Security and Threat Management Division
Ministry of Science and ICT
194, Gareum-ro
Sejong-si, 30121, Republic of Korea

Subject: Public Consultation on Amendments to Korea's Cloud Security Assurance Program (CSAP)

Dear Minister Lee and Director Heo:

The U.S. Chamber of Commerce ("U.S. Chamber") is the world's largest business federation, representing the interests of more than three million businesses and organizations of every size, sector, and region, including U.S. companies that have invested billions of dollars in Korea and support jobs for thousands of Korean citizens. We are strong supporters of a productive U.S.-Korea relationship, and our members represent the vital business community that contributes substantially to increasing jobs and growth in both Korea and the United States.

The U.S. Chamber and our U.S.-Korea Business Council ("USKBC") welcome the opportunity to respond to the Notification of the Security Certification for Cloud Computing Service ("Notification") that was officially adopted on January 31, 2023, following two amendment initiatives in recent months. We are deeply disappointed in the hasty implementation of the amendments, merely one day after the closing of the public comment period. We encourage regular and meaningful public-private dialogue and consultation periods, as well as consideration of industry comments during the planning, formulation, and implementation phases of policies. Good regulatory practices are fundamental to transparent governance and fair trade. We urge your Ministry to continue to engage with stakeholders as the Korea Internet & Security Agency prepares the implementation guidebook in the coming months.

As the Notification envisions a number of reforms concerning Korea's Cloud Security Assurance Program ("CSAP"), we appreciate the Korean government's efforts to make much needed reforms to digitally transform and modernize the public sector. However, these changes are insufficient to remove existing market access barriers and would not allow global cloud service providers ("CSPs") to compete on an equal footing in Korea's public sector cloud market. By requiring U.S. CSPs to build a separate Korea-unique product architecture to participate in the government procurement process, CSAP would represent a technical barrier to trade for U.S. firms. We reiterate the need for additional and robust stakeholder consultation throughout the CSAP reform process, given that the policy changes proposed to date fall short of our concerns and expectations.

As noted in our previous comments on the "*Guideline on the Use of Cloud Services for Critical Information and Communications Infrastructure in Private Sectors*," submitted on November 25, 2020, we strongly believe that a multi-stakeholder approach to cybersecurity is the most effective way to encourage economic activity while ensuring security, and that effective cybersecurity is fundamental to the resilience of digital infrastructure, digital trade, and the global value chain.

As the Korean government takes steps to reform CSAP and develops other policies associated with cloud infrastructure, its proposals should be made interoperable with international standards and the latest technological developments in the industry, and thereby better facilitate our shared goal of creating an inclusive, secure, open, and transparent digital ecosystem in Korea. In this context, we recommend the following:

1. Remove Personnel Presence Obligations: The Notification now requires the operations and management personnel of cloud service providers be located within the territory of Korea to obtain the low-tier certification. This unprecedented requirement would present significant regulatory challenges. Local presence obligations onerously discriminate against foreign companies by increasing compliance costs, which could lead to less foreign direct investment and a reduction in cloud related services. Furthermore, the local personnel requirement conflicts with the fundamental operational principle of cloud computing, given that cloud services can be provided on a cross border basis without restricting relevant personnel groups within a particular physical location. By nature, cloud computing services and technological offerings are globally deployed and scaled through the virtual space of the Internet. All major global CSPs, including Korea's leading CSPs, are not engaged in the practice of duplicating their management and operations personnel separately at each of their overseas operational sites. We urge the Korean government to clarify this obligation to ensure that cloud services can be provided on a cross border basis with the support of management and operations personnel outside of Korea to guarantee the resilience and security of the network and the necessary life cycle management of the cloud systems.

2. **Commit to Cross-Border Data Flows for Cybersecurity and Innovation, Subject to Appropriate Safeguards:** The free flow of data across borders is a prerequisite for a successful, innovative, and secure digital economy. Any measure that restricts data flows, such as the requirement for physical locations of cloud systems, backup systems, and data to be limited to Korea, may deter investment in Korea and limit its access to innovative digital tools and cross-border services, such as instant security patches and upgrades from cyber threats happening in other parts of the world or AI tools that require combining datasets with global datasets. Data localization also runs counter to the Korean government's ambitions to export information technology services, as localization measures act as a market access barrier and may violate obligations under the General Agreement on Trade in Services. In addition, data localization measures can increase the vulnerability of Korean users' data to security breaches (for instance, by limiting options on implementing data redundancy), as well as adversely affect Korea's investment environment. We therefore urge the Korean government to provide assurances that data may be transferred and processed outside of Korea, subject to appropriate safeguards, including encryption in-transit.

3. **Accept Alternative Security Certification Methods that Properly Reflect the Cloud Environment:** The recent revision of the CSAP Notification (from January 19, 2023) allows CSPs to obtain alternative security certification methods to Common Criteria under the Security Compatibility Validation Scheme ("보안적합성검증체계") controlled by the National Intelligence Service. However, there is still ambiguity on whether these alternatives would properly reflect the cloud environment. As background, the use of Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408-1) was designed with the assumption that security solutions are implemented in hardware form and has already proven to be difficult and costly to implement and attest use of its controls, especially for small and midsized enterprises. Consequently, it is not feasible to apply Korea's separate Common Criteria certification scheme to cloud environments, which are integrally configured using open-source software in a virtualized and distributed environment. We recommend the Korean government align with or mutually recognize alternative and more appropriate cloud services security certifications, such as FedRAMP.

4. **Avoid Fragmented Cloud Security Architectures:** The U.S. Chamber advises the Korean government to tailor cloud cybersecurity schemes in a manner that utilizes international standards based on levels of risk and size of organization. Public and private sectors benefit from policies that incorporate widely accepted and globally recognized industry-led cybersecurity frameworks, technical

specifications and international standards, such as, ISO/IEC 17788 and ISO/IEC 17000 and to a lesser extent ISO/IEC 9000 and ISO/IEC 27000, into any future policy enactments. Globally we have urged governments to avoid mandating local standards and controls that diverge from these international norms. International standards, such as the ones outlined above, are widely used by industry across global markets for cybersecurity of cloud services and are largely process-focused—designed to help organizations start a cybersecurity program or improve an existing one. Unnecessary divergence in the regulatory frameworks weakens our collective defenses, and advantages malicious cyber actors. As such, we support efforts aimed at aligning regulatory approaches across countries and promoting mutual recognition agreements to better reflect globally accepted best practices.

5. **Allow for Internationally Recognized Encryption Algorithms:** Cloud services procured by the Korean government are required to provide a certified national standard encryption technology that only supports a duplicative and local K-CMVP encryption algorithms. For many CSPs, this is impractical since they already use internationally recognized encryption algorithms in other markets for high-risk applications. We recommend that the Korean government recognize the FIPS 140-2 approved encryption algorithms, including AES256, a widely used algorithm in the list of verified encryption algorithms.

6. **Allow for Logical Separation for the Moderate Tier of Data Systems:** Current requirements allow for logical (vs. physical) separation for the low tier of CSAP certification, but not for moderate or high tier data systems. Physical network separation requirements undermine the functionality of cloud computing services while offering negligible enhanced security. We recommend that any requirements for physical network separation should be reserved only for high tier government workloads (e.g., national security) and not for low and moderate tiers of data systems. We welcome additional consultations with the Korean government to explain why logical separation may be more secure than physical separation and to provide examples of moderate-tier data systems in the United States that allow for both logical separation and cross border data flows.

7. **Consider the Use of Cloud Infrastructure as Critical for Zero Trust Networks:** After the Colonial Pipeline ransomware attacks in the U.S., a strong emphasis in public and private sectors has been made on segmenting operational technology and information technology systems, controllers, etc. Network and micro-network segmentation is a key pillar of the U.S. Department of Defense and the National Institute of Standards and Technology's guidance on zero trust architectures ("ZTA"). Network Segmentation is rapidly becoming an industry supported best practice, regardless of whether a system is classified as a highly sensitive or national security system or otherwise.

   It should be noted that the principles of network segmentation and ZTA do not exclude network policies from enabling data flows. Strong network segmentation

does *not* mean that data should be localized. In contrast, the best principles of Zero Trust Architecture prioritize accessibility to data at all times, from any location around the world, on a per session basis, based on strong identity management, and secure access. Use of cloud infrastructure is critical for zero trust networks.

8. **Establish Regular Dialogue on Cloud Services:** The U.S. Chamber and USKBC welcome the opportunity for regular dialogue with the Korean government regarding cooperation on cloud services and cybersecurity to share international best practices and support the Korean government's digital transformation initiatives.

The U.S. Chamber and USKBC value the Yoon administration's efforts to prioritize CSAP reform and initiate this process with the new opening at the low tier as a first step. Continued stakeholder consultation on the impacts of these policies will be critical, and the U.S. Chamber and USKBC welcome any opportunity to connect with your Ministry to discuss this issue in greater detail. Thank you for your consideration of our views, and we look forward to continuing our engagement. If you have any questions, please do not hesitate to contact me at ejelalian@uschamber.com or Abel Torres, Executive Director at the Center for Global Regulatory Cooperation, at atorres@uschamber.com.

Sincerely,

Esperanza Jelalian
Executive Director
U.S.-Korea Business Council
U.S. Chamber of Commerce

Cc: Mr. Park In-seok, Cyber Security and Threat Management Division, Ministry of Science and ICT
Mr. Song Kyucheol, Attaché for Science and ICT, Embassy of the Republic of Korea