U.S. Chamber of Commerce and U.S.-Korea Business Council
Recommendations on the Guideline on the Use of Cloud Services for
Critical Information and Communications Infrastructure in Private Sectors

November 25, 2020

The U.S. Chamber of Commerce (Chamber) and the U.S. Korea Business Council (USKBC) commend the Ministry of Science and ICT (MSIT) for launching the Guideline on Use of Cloud Services for Critical Information and Communications Infrastructure (CII) in Private Sectors (Guideline). Incorporating a wide range of stakeholder perspectives serves to enrich the quality of the draft. Technological integration and mass data storage via cloud sharing are becoming commonplace in business. We fully support the Korean government's efforts, given its significance, to establish new procedures, protocols and standards to ensure the safe, secure, and efficient use of cloud services, in addition to its role in supporting, promoting and attracting investments in the field of information technology.

The Chamber views the safe, secure and efficient use of cloud services a top priority. Businesses of all sizes are investing in effective cloud computing and cloud backup systems. With more companies and organizations tapping into the flexibility, agility and cost savings that come along with leveraging cloud service providers (CSPs) to support business operations and moving data to the cloud, there are new compliance risks and security threats to address. These must be adequately protected against if we are to ensure that the benefits from the digitization of our economies are not outweighed by the risk. However, these risks are not unique to one country, and policies to address these risks should not create barriers to trade and market access through unique regulations that risk stifling innovation and preventing companies from offering secure global solutions to their customers.

Governments and businesses face shared, cross-border challenges. Unnecessary divergence from international norms on regulatory frameworks government responses make our defenses weaker and our adversaries stronger. As such, we support international efforts aimed at aligning regulatory approaches to better reflect globally accepted best practices and standards. As Korean authorities further develop the Guideline and other policies associated with cloud infrastructure, we urge the Government of Korea to make these policies interoperable with the global standards to better facilitate our shared goal of creating an inclusive, secure, open, and transparent digital ecosystem in Korea.

The U.S. Chamber of Commerce and the USKBC recommend the following:

- **Align Use of Cloud Services with Existing International Best Practices:** A blanket recommendation that discourages the use of cloud services by critical information and communications infrastructure entities denies private sector organizations of the security and efficiency enhancements made possible by cloud technology. The Chamber and the USKBC therefore urge the Government of Korea to remove this recommendation. Additionally, country-specific compliance requirements and prior government approval for use of cloud services create a fragmented security approach and unnecessary operational overhead for critical information and communication infrastructure entities. Instead, the Chamber and the

USKBC recommend that the Guideline be based on industry-led international standards and frameworks. Private industry greatly benefits when governments incorporate existing cybersecurity frameworks, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework or the International Organization/International Electrotechnical Commission (ISO/IEC) 27001:2013, into any future policy enactments and avoid mandating local standards and requirements that diverge from these international norms. These frameworks are largely process-focused—designed to help organizations start a cybersecurity program or improve an existing one—and are applicable to cloud computing environments. There are several cloud specific security standards initiatives that have recently been published, including ISO/IEC 27017 and ISO/IEC 27018, that provide more detailed guidance and recommendations for both cloud service customers and cloud service providers.

- **Review and Harmonize Rules Across Korea's Executive Agencies:** As MSIT and the Financial Services Commission (FSC) develop and enforce their own technology requirements, the business community is often faced with duplicative and potentially conflicting rules and regulations. For example, the MSIT is considering designating cloud data centers as Critical Information Infrastructure (CII), which would be excessively burdensome for global cloud service providers. Similarly, the FSC announced recently that it will strengthen its on-site audit of cloud data centers despite preexisting on-site inspections required by other ministries. To promote the efficiency and security of cloud computing services in Korea, the Chamber and the USKBC request that the Korean government review and harmonize these requirements for cloud data centers. More broadly, the MSIT and FSC should review and harmonize their policies, laws, rules, and regulations to streamline business compliance and minimize their deviations from global standards.

- **Eliminate Protectionisms in Governmental Cloud Market:** The Ministry of Interior and Safety (MOIS) is planning to create a 'Private-Government Cloud Center Committee,' with only 10 domestic cloud CSPs, deliberately excluding global CSPs, for the full-scale transition of the government to the public cloud services. The USKBC and our members view Korea Internet & Security Agency's mandatory Cloud Security Assurance Program certification requirements, as a qualification for participation in the Committee, as a major trade barrier between Korea and the United States and as a discriminatory policy. The USKBC requests for MOIS to allow for the inclusion of global CSPs in the 'Private-Government Cloud Center Committee' and not pre-determine the number of CSPs that can qualify.

- **Commit to Free Flow of Data:** The flow of data across borders is a prerequisite for a successful and innovative digital economy. Any measure that restricts data flows will deter investment in Korea and limit its access to innovative digital tools and cross-border services. 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 (by, for instance, limiting options on implementing data redundancy), as well as

adversely affect Korea's investment environment. The USKBC therefore urges the Government of Korea to remove any references to local data storage requirements via the establishment of domestic facilities for cloud services and explicitly commit to the free flow of data.

- **Establish Regular Dialogue on Cloud:** The Chamber and the USKBC welcome the opportunity for regular dialogue with the Government of Korea regarding cooperation on cloud to share international best practices and support the Korean government's Digital New Deal program.

The Chamber and the USKBC appreciate the opportunity to share with you our primary concerns with the Guideline. We stand ready to work with the Government of Korea and key stakeholders and industry in ongoing consultations regarding new policies and sound policy implementations associated with cloud computing and cloud backup systems.

Thank you again for your time, and we look forward to continuing dialogue that helps achieve Korea's economic objectives and allows for increased American business activities in Korea. If you have any questions, please do not hesitate to have your staff contact USKBC Executive Director Esperanza Jelalian at ejelalian@uschamber.com.