SEPTEMBER 2, 2020

OVERVIEW OF THE U.S. CHAMBER AND USKBC DIGITAL POLICY PRIORITIES AND RECOMMENDATIONS

The U.S. Chamber of Commerce and the U.S.-Korea Business Council (USKBC) strongly support discussions led by the U.S. Department of State with government officials from the Republic of Korea (ROK) under the U.S.-ROK Information and Communications Technology (ICT) Policy Forum. Our members are pleased that the two governments are scheduled to convene virtually for the annual ICT dialogue next week based on their shared commitment to further cooperation and enhance the digital economy. The Chamber and USKBC believe that continued commitment to strong economic relations between the United States and the Republic of Korea help promote U.S. interests and objectives in East Asia and the Indo Pacific region.

The Chamber and USKBC appreciate the opportunity to provide feedback on critical commercial priorities and recommendations of American companies operating in South Korea. Our submission includes input we have received from our membership on key issues and concerns that the U.S. government can raise at the meeting with ROK officials. We look forward to continuing our engagement with the State Department.

I. Address Uncertainty, Market Access Concerns Regarding Amendments to the Telecommunications Business Act and the Network Act: In May 2020, South Korea amended its *Telecommunications Business Act* and *Act on the Promotion of Information and Communications Network Utilization and Information Protection* ("Network Act") to essentially hold global content, or value-added telecommunication service ("VATS"), providers liable for providing stable services to users. As written, however, the amendments target foreign companies operating in Korea while also harming Korean industry, including startups and small and medium-sized enterprises ("SMEs"). The requirement that VATS providers ensure network quality remains unclear and may create significant financial and technical obligations. Moreover, the requirement for foreign VATS providers to appoint a local representative also runs the risk of conflicting with obligations under the *U.S.-Korea Free Trade Agreement* ("KORUS"). Taken together, these provisions will negatively impact Korean consumers and Korea's ecosystem of startups, SMEs, and global companies, as it will deter new players and investments in innovative digital services. The Chamber and USKBC understand that there will be public consultation for the presidential decrees by October and look forward to weighing in on the need for clarity and legal certainty for U.S. businesses operating in Korea. A joint letter from the Chamber and the Information Technology Industry Council to the Korean National Assembly detailing our concerns is attached.

II. Closely Engage Korea's New Data Protection Authority: Earlier this year, Korea amended the *Personal Information Protection Act* ("PIPA"), with changes taking effect on August 5, 2020. Under the amended PIPA, the personal information supervision function that was previously shared and delegated through different ministries, such as the Korea Communications Commission, the Financial Services Commission, and the Ministry of the Interior and Safety, are now centralized in one data protection authority. The new Personal Information Protection Commission ("PIPC") has been elevated to a ministry-level agency under the Prime Minister's office that is exclusively responsible for personal information protection. The nine PIPC commissioners, led by Chairman Yoon Jong-in, will be comprised of government officials and various legal and policy experts.

The Chamber and USKBC support balanced, flexible approaches to the data protection that enable businesses to operate across markets.[1] The ability for businesses to transfer data out of Korea, efficiently engage regulators, and scale interoperable privacy practices are necessary in this regard. We welcome efforts by the Korean government to streamline Korea's data protection framework. We seek to strengthen our engagement with the PIPC as it issues new guidance on Korea's updated data privacy regime and to ensure it adopts non-discriminatory practices consistent with global standards. As in other markets, the Chamber and USKBC encourage the Department of Commerce and the Federal Trade Commission to build close collaboration with the PIPC on issues of data protection. We welcome opportunities to facilitate such dialogue.

III. Address Concerns about Unequal Access to Korea's Public Procurement Markets: Despite South Korea's commitments to open its government procurement to U.S. suppliers under the World Trade Organization's revised *Agreement on Government Procurement* ("GPA") and KORUS, U.S. businesses continue to face challenges accessing procurement contracts. Recent examples in the digital space include the Korean "Digital New Deal" projects and the Ministry of Interior and Safety's ("MOIS") Private-Government Cloud Center Committee ("Committee"). While Chamber and USKBC members are interested in participating in the digital projects under the "Korean New Deal" and in MOIS' newly established Committee tasked with facilitating the government's full-scale transition to cloud computing in the public sector, they face several challenges. First, the Korean government plans to give preferential treatment to domestic information technology ("IT") firms, particularly SMEs. This is also the case for the Committee, which includes only ten domestic cloud service providers ("CSP"s). Global CSPs are excluded from this Committee and from providing cloud services to the public sector because they have not been certified by the Korea Internet and Security Agency's Cloud Security Assurance Program ("CSAP"). CSAP represents a key trade barrier for U.S. CSPs, as noted in USTR's 2020 *National Trade Estimate Report*, as U.S. firms are unable to meet

[1] U.S. Chamber of Commerce, Privacy Principles.

some components of the certification without creating a separate, Korea-unique product.[2] To make matters worse, CSAP is currently expanding to other industries. The Korean Health and Medical Information Service recently introduced the CSAP certification criteria as a new requirement for medical institutions looking to adopt cloud-based Electronic Medical Record (EMR). Global cloud service providers operating in Korea are increasingly concerned that CSAP will become a norm in the public cloud market, with potential spillover to other industries. Second, in addition to CSAP, there are various regulations that discriminate against global IT firms in the public sector market, including the *Software Promotion Act*; the Ministry of Science and ICT's *Guideline for IT Network Equipment Construction*; and the National Intelligence Service's *Network Security Evaluation*, which act as *de facto* technical barriers by delaying the issuance of certificates.

Given these trade barriers, the Chamber and USKBC urge the Korean government to provide equal access for U.S. private sector participation in the government procurement markets, which would allow Korea to adopt the latest cutting-edge IT technology globally and to establish a strong alliance with the United States against growing international cyber security threats. We also encourage MOIS to level the playing field by allowing global CSPs to participate in the Private-Government Cloud Center Committee and the relevant Korean ministries and agencies to ensure fair competition between domestic and foreign companies in the public sector market.

IV. Promote Responsible Global Development and Deployment of 5G: It is important for governments to devote more resources to the promotion of industry leadership in the development of standards, intellectual property, and patents that are essential to the deployment of an open technologies-based, secure, and trusted 5G ecosystem.

The Chamber urges governments to take the following actions:

1. Support investments in research.
2. Uphold fair processes in standards-setting bodies.
3. Accelerate deployment of all technologies that will support the 5G ecosystem.
4. Provide strong intellectual property rights for innovators.
5. Help allies see a larger market for trusted vendors.
6. Facilitate the transition to interoperable technology-neutral solutions.

Our members share the U.S. government's concern that there is no place for untrusted vendors in any part of 5G networks, *i.e.*, in the core, radio access network (RAN), or edge. Further, we believe that the U.S. government and its traditional international allies can – and must – foster trust and improve security through continued engagement with the private sector

[2] Office of the U.S. Trade Representative, 2020 National Trade Estimate Report on Foreign Trade Barriers

on technical and nontechnical risk identification and mitigation efforts, as well as the promotion of continued development of trusted 5G technologies, services, and products.

The U.S. government should continue to urge the Korean government to establish clear public policies aimed at accelerating the development and voluntary adoption and use of virtual, open, and interoperable 5G technologies and solutions both domestically and internationally, particularly for the O-RAN standard. Open standards are developed through a recognized industry-led, consensus-driven solution and establish protocols and form foundations that make applications more functional and interoperable. The O-RAN standard not only streamlines the development and deployment of open technologies-based 5G, but it removes barriers stemming from vendor lock-ins that impede data exchange and interchange. The O-RAN standards will lead to an interoperable, software-defined network architecture and will benefit consumers, competition, the economy, and national security.

V. Advance Risk-Based Approaches to Cybersecurity: The Chamber and USKBC recognize that managing cyber risk, especially with regard to critical infrastructure, is vital to the economic and national security of the United States and Korea and increasingly important for our nations bilateral digital trade relationship. As such, we urge both governments to:

1. Build cyber capacity with respect to national competent authorities, legal conventions (including the Budapest Convention on Cybercrime), computer emergency response teams, critical infrastructure protection, and cyber education.

2. Strengthen existing collaboration mechanisms for cooperating to identify and mitigate malicious intrusions or dissemination of malicious code that affect electronic networks, and use those mechanisms to swiftly address cybersecurity incidents, as well as for the sharing of information for awareness and best practices.

Cybersecurity threats continue to rapidly evolve and are increasing in scale, frequency, complexity, and consequence. The Chamber and USKBC believe that a risk-based approach is more effective to manage cyber risk than prescriptive regulation. We urge both governments to employ, and encourage enterprises within their territories to use, risk-based approaches that rely on consensus-based standards and risk management best practices to identify and protect against cybersecurity risks and to detect, respond to, and recover from cybersecurity events. Cybersecurity regulations shall to the maximum extent possible be aligned with risk-based approached best exemplified by the U.S. National Institute of Standards and Technology's Cybersecurity Framework or sector specific profiles such as the Financial Services Sector Cybersecurity Profile.[3]

[3] U.S. National Institute of Standards and Technology's Cybersecurity Framework; Financial Services Sector Cybersecurity Profile

VI. Review and Harmonize Rules Across Korea's Executive Agencies: As the Ministry of Science and ICT ("MSIT") and the Financial Services Commission ("FSC") develop and enforce their own technology requirements, the business community is often faced with duplicative 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 CSPs. 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 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.

VII. Strengthen Dialogue Between the United States and Korea on AI: South Korea's National Assembly passed the *Framework Act on Intelligent Informatization* in May 2020, paving the way for its enforcement in December 2020. The Act stipulates a mandatory "social impact analysis" on artificial intelligence ("AI") services and a possible review of the legal liability regime for AI. The Act is still high-level, and the government is currently drafting the subordinate decree and guidelines. The U.S. Government should urge Korea to adhere to global standards, including the Organization for Economic Cooperation & Development's AI Recommendations, and engage with the U.S. business community before taking additional actions on AI governance. The Chamber and USKBC also encourage both governments to consult our *Principles on Artificial Intelligence* for best practices on AI policy.[4] The Chamber and USKBC will be monitoring developments in this space closely as it could lead to burdensome regulations regarding AI technology and services.

VIII. Strengthen U.S.-Korea Engagement in ITU – World Telecommunication Standardization: The ITU plays a vital role in the allocation of spectrum, developing specific technical telecommunication/ICT standards, and promoting the growth of connectivity in developing countries, the WTSA-20 presents an opportunity for the U.S. government and our allies, including Korea, to ensure that the ITU does not expand its jurisdiction and remains focused on its existing mandate and core competencies. Many of the emerging technology initiatives being promoted by some ITU members are duplicative of ongoing industry-led initiatives and standards activities (please see WTSA consultation attachment). In 5G, these activities are already contemplated. For example, standards development process at the 3rd Generation Partnership Project (3GPP), specifically through SA WG3, which is responsible for determining the security and privacy requirements and specifying the security architectures and protocols. The smart development of international standards for 5G deployments, such as the 3GPP and progress by the Open Radio Access Network (O-RAN) Alliance, advance commercial and security priorities.

[4] U.S. Chamber of Commerce, Artificial Intelligence Principles.

ABOUT THE U.S. CHAMBER OF COMMERCE

The U.S. Chamber of Commerce is the world's largest business federation representing more than three million enterprises of all sizes and sectors. The Chamber is a leading business voice on digital economy policy, including on issues of artificial intelligence, data privacy, cybersecurity, digital trade, and e-commerce. In the United States and globally, we advance sound policy frameworks that support economic growth, promote consumer protection, and foster innovation.

ABOUT THE U.S.-KOREA BUSINESS COUNCIL

The U.S. Chamber of Commerce's U.S.-Korea Business Council (USKBC) is the premier business advocacy organization in Washington representing top U.S. companies engaged with South Korea. The Council is made up of senior-level executives of U.S. companies from every business sector that are major investors in Korea and are actively committed to the Korean market.

USKBC MISSION STATEMENT

Established in 1987, the USKBC seeks to enhance business ties between the United States and South Korea, as well as to promote the bilateral economic and political relationship in order to expand trade and investment between the two countries.

For any questions or inquiries regarding this submission, please contact USKBC Executive Director Esperanza Jelalian at ejelalian@uschamber.com.

Attachments:

- U.S. Chamber of Commerce and USKBC Submission on Amendments to the Enforcement Decree of the Amended Personal Information Protection Act (May 8, 2020)
- U.S. Chamber of Commerce and Information Technology Industry Council Letter to the Legislation and Judiciary Committee of the National Assembly of South Korea (May 15, 2020)
- U.S. Chamber of Commerce Submission to the National Telecommunications and Information Administration's request for public comment (RFC) on Input on Proposals and Positions for the 2020 World Telecommunication Standardization Assembly (June 2020)