Computer & Communications Industry Association
Open Markets. Open Systems. Open Networks.

Ministry of Science And ICT

Government of the Republic of Korea

Seoul, Republic of Korea

Via electronic mail: emeaning@korea.kr

26 February 2024

Re: Announcement No. 2024-0092 - Revision of Notice on Security Certification of Cloud Computing Services

To whom it may concern:

The Computer & Communications Industry Association (CCIA) submits the following comments regarding the Ministry of Science and ICT (MSIT) proposed revisions of the Notice on Security Certification of Cloud Computing Services, amending the requirements finalized January 31, 2023 which governs the Cloud Security Assurance Program (CSAP). CCIA is an international, not-for-profit trade association representing a broad cross section of communications and technology firms.[1] CCIA appreciates the opportunity to provide its views in this consultation.

Introduction

CCIA welcomes MSIT's decision to revise requirements that cloud service suppliers must meet to offer cloud computing services to the public sector in Korea. CCIA also supported MSIT's introduction of a risk-based approach to certification, and the tailoring of requirements to the distinct risk categories of low, medium, and high risk.

Although the revised requirements for low-risk categories of data provided some modest improvements to the certification scheme[2] the revisions ultimately failed to address several

[1] For fifty years, CCIA has promoted open markets, open systems, and open networks. The Association advocates for sound competition policy and antitrust enforcement. CCIA members employ more than 1.6 million workers, invest more than $100 billion in research and development, and contribute trillions of dollars in productivity to the global economy. For more, visit www.ccianet.org.

[2] Key improvements to low-tier certification included allowing for logical versus physical separation for public sector data, and flexibility on location of computing resources.

other key barriers preventing the Korean public sector from accessing services offered by trustworthy foreign suppliers. As a result, it is unclear whether even a single foreign supplier has so far succeeded in qualifying to offer such services, even at the low-risk level.

The current proposed set of amendments that is the subject of this consultation does nothing to remedy the unreasonable requirements still applicable to low-risk applications (use of national encryption and National Intelligence Service (NIS) certification). These proposed amendments not only extend these requirements to mid- and high-risk data, but they also remove for mid and high tier services the two improvements applied to data in the low-tier (the possibility of logical versus physical separation of data, and flexibility on location of resources). As a result, these proposed amendments will lock in requirements applicable to nearly all public sector cloud computing contracts and only further isolate Korea's public sector from the most competitive, innovative, and best-in-class services. The key restrictions proposed for mid- and high-tier data include requirements to:

- physically separate facilities used for servicing the public sector from those servicing commercial customers (which was allowed for low-tier data);
- exclusively use equipment, resources, and personnel located in Korea;
- exclusively store data in Korea;
- exclusively utilize Korea's national encryption algorithms; and
- exclusively rely on NIS certification for key infrastructure.

It is highly disappointing that MSIT proposes to maintain these restrictions. The Korean government's decisions with respect to these proposed amendments will determine whether Korea's public sector has access to state-of-the-art cloud systems addressing two key capabilities: innovation and security.

Cloud computing suppliers that provide the most advanced technological capabilities are critical for the Korean economy as it looks to leverage innovative applications in governmental programs, including rapidly-developing artificial intelligence applications, for which cloud computing is a foundational capability. In addition, Korea's unique geopolitical challenges also demand robust cybersecurity as well as interoperability with allied defense systems. The former is fundamental to the resilience of the country's digital infrastructure and ongoing digital transformation. The latter is necessary as Korea becomes more interlinked in national security cooperation along with countries such as the United States and Japan. In all of these areas, U.S. firms offer unparalleled capabilities; blocking their ability to offer such services, while perhaps beneficial for competing Korean suppliers who advocate for their maintenance, is unlikely to reflect Korea's broader economic or security interests.

Korea's effective exclusion of U.S. cloud computing firms from the country's rapidly growing public-sector market for such services risks violating Korea's government procurement obligations under both the WTO and Korea-U.S. Free Trade Agreement (KORUS).[3] The overall goal of these obligations is to ensure both *de facto* and *de jure* national treatment - the ability of foreign suppliers to compete fairly with local competitors. One specific obligation that procurement rules impose is a commitment of a Party not to use technical specifications "...with the purpose or the effect of creating unnecessary obstacles to international trade[4]." (Article X.1). Given the current inability of top global suppliers to access this market, Korea is not meeting that standard, and this amendment process is an important opportunity to rectify that deficiency in this certification scheme.

Comments on specific provisions

Specific provisions of the amended notice are addressed below, in the order presented. All of these requirements are documented in Appendix 4 of the proposal, released here, under Attachment 2.

Article 14.1.2 - certification of computer equipment

Equipment certification procedures are typically designed to ensure the confidentiality, integrity and availability of data, and services dependent on such data, through defined technical requirements and conformity assessment procedures. A key mechanism for meeting these goals, while facilitating trade between trusted partners has been use of international standards, such as the well-established Common Criteria testing program. This program, standardized internationally as ISO 15408, and implemented through labs accredited in multiple jurisdictions, is one of the few globally recognized programs for mutual recognition of test results. Korea participates in this program, which is the basis for many Korean products to be sold to the U.S. public sector. Nonetheless, Article 14.1.2 specifies that for all three risk categories that equipment must be certified by the NIS. This is redundant for those suppliers who have invested significantly in the robust testing and certification that allow them to sell globally, including to all OECD countries. In amending CSAP, this requirement should be made optional for those firms who can demonstrate compliance with comparable standards and conformity assessment procedures, including under Common Criteria.

---

[3] In both agreements, Korea committed to allow U.S. suppliers rights to access, on a national treatment basis, the whole computer services sector (CPC 84). See: https://e-gpa.wto.org/en/Annex/Details?Agreement=GPA113&Party=Korea&AnnexNo=5&ContentCulture=en

[4] See WTO Agreement on Government Procurement, Article X.1, at: https://www.wto.org/english/docs_e/legal_e/rev-gpr-94_01_e.htm

Article 14.2.1 - Physical Location and Isolation

Physical location

Article 14.2.1 requires that all systems, backup systems, data, and management and operational personnel relating to mid-and high-tier services be located exclusively in Korea.

Since competing Korean suppliers have built their systems in Korea using local personnel, this requirement poses no undue burden to local suppliers. It is, however, a form of *de facto* discrimination against foreign suppliers, for whom many key resources are not located in Korea. While most major U.S. cloud suppliers have made significant infrastructure investments in Korea, including building data centers with advanced functionalities, being able to rely on global resources is a key advantage they offer and a key benefit to Korean public sector customers. Accordingly, access to the best engineering talent; the most comprehensive cybersecurity monitoring systems (offering global visibility into emerging threats); and back-up systems distant from the persistent threats Korea faces, are all capabilities the Korean government should embrace and promote. While this is another example of requirements that local suppliers may support as an effective form of protection from competition, trustworthy foreign-affiliated systems can offer resiliency that a Korea-only system cannot.

In short, prohibiting access to global resources and back-up data storage increases risks to public sector customers and should be removed.

Isolation

Korea is unique among OECD countries in requiring the physical separation of cloud computing facilities used to serve the public sector for the majority of such contracts–*i.e.,* those categorized as mid-tier in terms of sensitivity. It is now well established that robust security can be achieved in all but the most sensitive service, without relying on physical isolation. By way of comparison, under the United States' well-established certification program called FedRAMP, over 75 percent of authorizations are for mid-tier services, and of those, about 40 percent are offered either through a public or hybrid cloud model–*i.e.*, where full physical separation for cloud computing workloads is not a requirement.[5] In fact, under FedRAMP,

[5] See https://marketplace.fedramp.gov/products

hundreds of authorizations, some even at high-level of sensitivity, are offered in this manner, clearly demonstrating that security is not inextricably tied to physical separation.

The reason public cloud offerings persist in the public sector United States is instructive: in most cases, public cloud offerings are often implemented in a most cost-effective and more flexible manner, enjoying superior economies of scale and a faster integration of the most advanced technologies. These factors that can put services offered through dedicated facilities at a disadvantage, an outcome Korea is likely to bring on itself, if its rigid preference for physical separation continues to prevail.

While there may be specific services at a high-tier of sensitivity that benefit from dedicated facilities, mandating this requirement as a condition of offering any mid- or high tier service denies the Korean public sector customers valuable capabilities. This is a form of *de facto* discrimination, putting non-Korean suppliers at a significant competitive disadvantage to local suppliers, and denies the Korean public sector the capabilities they offer. In addition, as an unjustified technical requirement, this requirement runs afoul of Korea's government procurement obligations cited above, the prohibition on using technical specifications "…with the purpose or the effect of creating unnecessary obstacles to international trade.[6]"

Article 14.2.1 mandates physical separation not only for processing, but for back-up storage as well. In amending CSAP, this physical separation requirement should be removed as an absolute requirement, for both mid- and high-tier services.

Article 14.3.1 - Verified Encryption Technology

Mandating the use of national standards for encryption (*e.g.,* SEED or ARIA) is a longstanding barrier that Korea has maintained in various public sector systems. Although ARIA, a cipher derived from the more widespread AES cipher, has been standardized in the IETF, its use is virtually non-existent outside of Korea. By contrast, manufacturers, software developers, and governments around the world have increasingly adopted the *de facto* global standard, AES (a cipher originally developed in Belgium, and adopted in the United States only after a rigorous competition between competing ciphers). Korean manufacturers are a major beneficiary of this trend, as products sold globally ranging from cell phones, tablets, computers, routers, and base stations rely on this technology to offer secure communications. Not only do global manufacturers and service suppliers overwhelming rely on AES, but so too do many of the

[6] See *supra*, note 3.

most security-conscious governments in the world: the United States,[7] the EU,[8] Germany,[9] France,[10] the United Kingdom,[11] Australia,[12] Canada[13] and Japan.[14]

Given the fact that ARIA is virtually unused outside of Korea, the ecosystem of hardware and software developers, manufacturers, and the services implementing such technology (computer services, banks, telecommunications service suppliers, etc.) is largely lacking, since it would be overly burdensome to develop an expertise relevant only for Korea. Accordingly, mandating this encryption technology puts foreign suppliers at a significant competitive disadvantage. In fact, forcing the use of a niche technology in the Korean market creates a protected Korean expertise that relies on this mandate. If this technology did not have equivalent options that were also subject to international standards, mandating its use might be justified. But, there are clearly equivalents; and thus, as with several of the requirements noted above, it is a requirement inconsistent with Korea's obligations to avoid technical requirements adopted for the "purpose or the effect of creating unnecessary obstacles to international trade."[15]

In amending CSAP, the requirement to use national Korean encryption should be removed as a requirement for all risk categories.

Conclusion

If Korea hopes to meet its goal of embracing cloud computing in the public sector as a means of promoting more efficient, innovative and secure government services, the proposed CSAP amendments are a major step backwards. They also call into question Korea's compliance with its international trade obligations, under both the WTO Government Procurement

---

[7] See https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197-upd1.pdf

[8] See https://www.enisa.europa.eu/publications/algorithms-key-sizes-and-parameters-report/@@download/fullReport

[9] See https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf?__blob=publicationFile

[10] See https://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_B1.pdf

[11] See: https://www.ncsc.gov.uk/collection/device-security-guidance/security-principles/protect-data-at-rest-and-in-transit

[12] See https://apo.org.au/sites/default/files/resource-files/2018-12/apo-nid208151_1.pdf

[13] See Cryptographic algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information - ITSP.40.111 - Canadian Centre for Cyber Security

[14] See https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2012r7.pdf

[15] See *supra*, note 3.

Agreement and KORUS. For these reasons, as detailed above, CCIA strongly urges the Korean government to reconsider its approach.