Business Software Alliance

Updated Concerns Regarding Korea's Cloud Security Assurance Program (CSAP)

February 25, 2026

The Honorable Rick Switzer
Deputy United States Trade Representative
The Honorable Ken Schagrin
Assistant United States Trade Representative

Office of the US Trade Representative
600 17th Street, NW
Washington, DC 20508

We welcome your efforts to resolve unfair and non-reciprocal trade barriers that hurt US strategic interests, US companies, and US workers. The Business Software Alliance (**BSA**)[1] takes this opportunity to provide you with updated information on South Korea's Cloud Security Assurance Program (**CSAP**), which the Government is reportedly planning to modify in ways that risk further eroding US exporters' access to the Korean market. This submission builds on BSA submissions from March, July, and October 2025, as well as Global Data Alliance submissions from July and October 2025.

As discussed below, we urge USTR to continue engaging with Korea to ensure that any restructuring of the CSAP results in genuine market-opening reform rather than a repackaging of existing restrictions. Addressing such a longstanding market barrier would advance US commercial interests and send a clear signal that the US is committed to confronting discriminatory trade practices. In particular, Korea should:

1. Classify a larger share of public institution data systems as Low tier and remove references to personal information in the CSAP.
2. Align certification requirements for Low and Medium grade data systems with international best practices by eliminating requirements for physical network separation, data residency, use of Korea-developed encryption algorithms, and local personnel presence.
3. CSAP should also accept internationally recognized standards and certifications from internationally accredited bodies.

This letter is accompanied by three Annexes. **Annex I** describes the most recent CSAP amendment proposals from late 2025 and early 2026. **Annex II** describes how the CSAP has effectively prevented US CSPs from accessing Korea's public sector market. **Annex III** explains why CSAP reform efforts to-date have been insufficient in addressing the core issues that continue to impede market access.

We have consistently raised these same concerns directly with authorities in Korea, including in repeated meetings in Seoul. Unfortunately, we have not found the authorities to be responsive to our concerns.

BSA and its affected member companies would appreciate the opportunity to meet (virtually) with your staff to discuss these concerns. Please let us know if you have any questions or comments.

Annex I – Proposed CSAP Amendments Will Worsen US Access to the Korea Cloud Marketplace

The CSAP was developed to ensure that Cloud Service Providers (**CSPs**) serving the public sector meet the appropriate security requirements. However, in practice, the CSAP imposes technical requirements that severely restrict most CSPs, including nearly all foreign CSPs, from offering meaningful cloud-enabled services to public entities in Korea. CSAP has long been identified as a trade barrier in the USTR National Trade Estimate Report on Foreign Trade Barriers.[2]

Recent reports suggest that Korea is planning to make CSAP more harmful to US exporters – expanding its scope from the public sector to the private sector, and increasing power of protectionist agencies in administering the Program.[3] Based on these developments, we highlight the following:

- The CSAP will reportedly be reframed as a "voluntary" certification for cloud procurement in the *private* sector.
- At the same time, responsibility for public sector cloud security procurement will be led by the National Intelligence Service (**NIS**), making the NIS the single authority responsible for approving cloud services used by the Korean public sector.
- NIS will absorb most or all existing CSAP security requirements into a new NIS-led framework for public sector cloud procurement, leading to a more – not less – protectionist approach.

These developments are concerning for the following reasons:

- **First,** expanding the reach of CSAP from the public sector to the private sector is a major step backwards. This move will extend CSAP's protectionist "digital sovereignty" features from the public sector cloud market to the much larger private sector cloud market.

  We also dispute the suggestion that this is an innocent change because CSAP will only exist as a "voluntary" certification mechanism. Korea has done nothing to eliminate the distortive and discriminatory Korea-unique technical requirements from CSAP. Moreover, extending CSAP into the private sector creates a pathway for these requirements to spread into regulated areas such as healthcare and education, where standards can become de facto requirements through sectoral rules or incentives.[4]

- **Second,** consolidating final approval authority under the NIS does nothing to remove the most problematic aspects of CSAP from the program. If anything, centralizing discretion in this national security agency means that CSAP will be administered with **less** consideration of Korea's obligations to the United States under KORUS and the WTO Agreements. This means less transparency and less predictability, coupled with more emphasis on infrastructure-based or sovereignty-related conditions, including domestic data center expectations**.** Reports have indicated that CSPs without domestic data centers will likely face significant difficulty competing for projects involving sensitive data, given concerns about on-site inspections and control.
- **Third,** US CSPs have already made significant investments to obtain CSAP's lowest-tier certification as the only viable entry point into Korea's public-sector market, including establishing substantial in-country capabilities to satisfy Korea-specific security conditions. Replacing CSAP with a new NIS-led regime featuring revised requirements would impose renewed compliance burdens and regulatory uncertainty after substantial sunk costs have already been incurred.

Annex II: How the CSAP prevents US CSPs from accessing Korea's public sector market

The CSAP was created by the Korea Internet and Security Agency in 2016 and elevated from administrative guidance to a legal requirement through a March 2022 revision to the Cloud Computing Promotion Act. The CSAP, which applies to Korea's central, provincial, and local public sector with very limited exceptions, presents significant barriers to US CSPs seeking to enter Korea's public sector. US CSPs are required to fulfill technical and administrative requirements, many of which are not in line with global standards and business practices, and which do not lead to improved cloud security:

A) **Physical Network Separation.** Most public sector data systems are required to be hosted on infrastructure and networks that are physically separated from those used by other clients. This requirement diverges from international best practices, which recognize logical separation as a secure and effective method for isolating sensitive workloads in multi-tenant cloud environments. While a few countries retain physical network separation requirements for some highly sensitive areas (national security, defense), it is rarely applied throughout the public sector, including to institutions that handle non-sensitive or even public data, such as public universities.

B) **Encryption.** CSPs are required to use Korean-developed encryption algorithms (e.g., ARIA, SEED). 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. After substantial advocacy efforts, Korea's National Intelligence Service (**NIS**) indicated in September 2024 that it will relax encryption requirements up to the Medium tier. There remains significant ambiguity regarding how this will be implemented in practice. To date, no formal updates or amendments have been made to the CSAP to reflect this change, leaving US CSPs in a state of legal and operational uncertainty.

C) **Data Localization.** All data associated with public sector data systems must be physically located in Korea. This is an unnecessary barrier for many US CSPs that store and process data in regional data centers outside of Korea. In some cases, the use of offshore data centers ensures redundancy and back-up. In cases of serious physical damage or cyberattack on one data center, data stored in physically remote data centers can be used to recover from the incident.

D) **Local Personnel Requirements.** CSPs must have operations and management personnel located within Korea to obtain CSAP certification. Local personnel requirements disadvantage US CSPs by significantly raising their compliance costs, as they must duplicate personnel and infrastructure already managed efficiently at scale elsewhere.

These requirements do little to enhance security while undermining the main benefit of cloud computing services provided by US CSPs, which is the economy of scale and state-of-the-art security capabilities of a globally-deployed cloud service. The CSAP continues to place US CSPs at a competitive disadvantage to domestic competitors and limits progress on the broader US digital trade agenda.

Annex III: Why CSAP reform efforts to-date are insufficient

In 2022, Korea began a review of the CSAP with a view to reform it in ways that would open market access possibilities for foreign CSPs. The Korean Government indicated it would benchmark CSAP to the US Federal Risk and Authorization Management Program (**FedRAMP**). In 2023, Korea introduced a three-tiered scheme dividing all public sector data systems into three tiers: Low, Medium, and High. However, these reforms are insufficient and still present significant challenges for US CSPs seeking to enter the public sector market in Korea:

- Most public-sector data systems continue to be classified as either Medium or High tier systems, for which US CSPs are unable to get certified. The Low tier only covers data systems which are open, public, and do not contain any personal information, which is a very narrow subset of public sector data systems. Specifically, if a public institution's data system contains personal information, which is broadly defined in Korea's Personal Information Protection Act (**PIPA**), it would be classified as either Medium or High tier. As such, even if a US CSP is CSAP-certified for Low tier data systems, it is still excluded from the majority of public sector opportunities in Korea, as it cannot serve institutions that handle even minimal amounts of personal information. Further, only CSPs that are CSAP-certified for the Medium or High tiers are cleared to participate in the Korean Government's digital transformation initiatives.
- Even for the Low tier, most of the requirements highlighted in Annex I continue to apply. The requirement to use physical network separation no longer applies to Low tier systems, allowing CSPs to use logical network separation to keep the public sector data systems distinct from those of their other customers. However, all three levels of CSAP classification, including Low tier, continue to require CSPs to use only Korea-developed encryption algorithms, physically locate data in Korea, and maintain local personnel presence.
- To date, only three US CSPs are CSAP-certified, and only for the Low tier. This outcome highlights the general ineffectiveness of Korea's limited reforms. Despite repeated claims of progress, the CSAP framework remains structurally protectionist and functionally inaccessible to US CSPs.

The continued lack of meaningful market access for US CSPs underscores the need for sustained and elevated US Government advocacy. Korea's piecemeal and limited adjustments have failed to address the fundamental structural barriers that prevent US CSPs from competing on fair and equal terms in the public sector market. The CSAP remains a significant non-tariff barrier for US CSPs. In the ongoing negotiations with Korea, the US should extract explicit and enforceable commitments from Korea to align the CSAP with global norms and enable market access for trusted US CSPs. These commitments should include the following:

1. Classify a larger share of public institution data systems as Low tier and remove references to personal information in the CSAP.
2. Align certification requirements for Low and Medium tier data systems with international best practices by eliminating requirements for physical network separation, data residency, use of Korea-developed encryption algorithms, and local personnel presence. CSAP should also accept internationally recognized standards and certifications from internationally accredited bodies.

[1] The Business Software Alliance (www.bsa.org) is the global trade association of the enterprise software industry, representing companies that are leaders in artificial intelligence, cybersecurity, cloud computing, and other cutting-edge technologies. For more information on the trade barriers discussed in this submission, *see*: (1) BSA Comments for National Trade Estimate Report on Foreign Trade Barriers, October 2025, https://www.bsa.org/policy-filings/us-bsa-comments-for-national-trade-estimate-report-on-foreign-trade-barriers; (2) BSA Submission to USG on Korea Cloud Security Assurance Program, July 2025, https://www.bsa.org/policy-filings/us-bsa-submission-to-usg-on-korea-cloud-security-assurance-program; and (3) BSA Comments to USTR on Unfair Trade Practices, March 2025, https://www.bsa.org/policy-filings/us-bsa-comments-to-ustr-on-unfair-trade-practices.

[2] US Trade Representative 2025 National Trade Estimate Report on Foreign Trade Barriers, p. 251 at 2025NTE.pdf.

[3] https://www.yna.co.kr/view/AKR20260130133600017?input=1195m; (2) "Public Cloud Certification to Move under NIS. Potential Implications for US-Korea Negotiations" by Korea Economic Daily, February 2, 2026, https://www.hankyung.com/article/2026020164411; (3) "NIS to Lead Public Cloud Oversight. Domestic Data Center Requirements Still Key" by News1, February 4, 2026, https://www.news1.kr/it-science/general-it/6060442.

[4] The Government has a precedent of introducing CSAP-like controls in sectors such as healthcare. For example, the Ministry of Health and Welfare imposed cloud security and infrastructure-related conditions on electronic medical record (**EMR**) systems used by medical institutions, including requirements tied to domestic hosting, certification, and compliance with Korea-specific security standards. Although not formally labeled as CSAP, these measures mirror key CSAP elements and have been linked to reimbursement eligibility and related policy incentives, effectively creating a de facto requirement for cloud services operating in the healthcare sector.