The Honorable Gina Raimondo
Secretary
U.S. Department of Commerce
1401 Constitution Avenue NW
Washington, DC 20230

The Honorable Antony Blinken
Secretary
U.S. Department of State
2201 C Street NW
Washington, DC 20520

The Honorable Katherine Tai
U.S. Trade Representative
600 17th Street NW
Washington, DC 20508

May 25, 2023

Dear Secretary Raimondo, Secretary Blinken, and Ambassador Tai:

On behalf of the undersigned associations, we write to raise concerns ahead of the upcoming meeting of the EU-U.S. Trade and Technology Council (TTC) taking place in Sweden at the end of this month, regarding new and alarming revisions to the European Commission's proposed European Cybersecurity Certification Scheme for Cloud Services (EUCS). We urge the United States to use upcoming meetings to engage with the European Commission and Member States to secure a durable solution that will enable American and European companies to compete on a level playing field, underpinned by transatlantic trust and safety, by removing nationality-based ownership restrictions of this draft measure.

EUCS is part of a broader concerted effort by Europe to enact a "digital sovereignty" agenda that seeks to disadvantage U.S. firms for the benefit of local alternatives, potentially threatening U.S. economic and national security interests. This agenda includes initiatives that mirror the discriminatory aspects of the EUCS, including parts of the EU's proposed Data Act.

Collectively, our member firms represent companies of all sizes across the economic spectrum that develop, sell, or rely on services and digital technologies in both the U.S. and European markets, and who employ tens of thousands of workers in the United States and Europe. Our associations have been engaged on the proposed EUCS scheme over the past year, urging policymakers to adjust the proposal so as not to undermine the market access rights U.S. cloud providers have relied on for the past decade that have supported significant investments in Europe, its economies and employment. Specifically, we have called for removing discriminatory ownership requirements that would prevent American cloud service providers from bidding on public sector and critical infrastructure cloud contracts across Europe.

While we support the overall goal of the EUCS to unify and harmonize the best security practices while reducing market barriers for businesses, we continue to be concerned about lack of transparency and public consultation, and the missing market impact assessment. For example, EU financial institutions and associations have voiced concerns that the so-called "sovereignty requirements" in EUCS would limit technology choice and be detrimental to the resilience and cybersecurity of digital and cloud solutions. Furthermore, the sovereignty requirements in EUCS appear contradictory to the recently adopted Digital Operational Resilience Act (DORA).

A recent leaked draft of the EUCS indicates that the new framework is going in a more problematic direction.[1] The leaked EUCS draft builds on one of the options advocated by France, which recently established its own national cloud security certification scheme (SecNumCloud), which shuts out American cloud services providers (CSPs) from bidding on French public sector contracts unless they enter minority joint ventures or transfer technology to French companies.

While the leaked ENISA draft of the EUCS has similarities with France's scheme, it differs importantly in scale and scope. The EUCS would apply to public and, potentially, private sector contracts affecting thousands of agencies and businesses across all 27 Member States. It relies on ill-defined categories of cloud workloads, and creates a new category of "high-risk" services (Evaluation Level 4), which includes the discriminatory ownership and control requirements (i.e., CSPs cannot be under "effective control" of a non-EU company and its global headquarters must be in the EU). Unfortunately, this new category does not serve to narrow the scope of discrimination, but, rather, enlarge it, through a definition of risk that is so elastic as to justify almost any tender as ineligible for a foreign-based bidder.

Indeed, "sovereignty requirements" may be required in various business and government contexts, for a very broad set of workloads, including data related to the protection of privacy, to medical secrecy, and to trade secrets, which includes the secrecy of production methods, economic and financial information, and of information on commercial or industrial strategies. While such categories of services do reflect real sensitivities, they correspond to common risks global certification schemes that advanced countries have long addressed through various forms of mitigation (e.g., encryption), without requiring discrimination with respect to the nationality of the supplier.

Such a broad category of services reserved for EU-based suppliers risks splintering the common market, and is almost certainly inconsistent with the EU's national treatment obligations under the World Trade Organization (WTO) Government Procurement Agreement (GPA) and the General Agreement on Trade in Services (GATS). Practically speaking, what this would mean is a Chinese-like model that would require American companies to relinquish ownership and operations of infrastructure to local sellers of record.

Strong and timely U.S. engagement on this issue is critical as the leaked EUCS draft will serve as a basis for further discussion among Member States, including during the May 26 European Cybersecurity Certification Group meeting.

[1] https://subscriber.politicopro.com/f/?id=00000188-06ec-deac-a39a-4fecbb520000

Specifically, we encourage the European Commission and Member States to remove entirely from the EUCS Evaluation Level 4, including the Annex J titled "Protection of European Data against Unlawful access." By removing discriminatory ownership and control requirements, the Commission can future-proof the EUCS and make it compatible with the EU's international trade obligations and obtain wide Member State support. The final version should be WTO-consistent and not require additional, complex legal and non-technical assessment and implementation procedures. If a mutually agreeable solution cannot be reached, we urge the U.S. government to seek WTO consultations with France on its SecNumCloud scheme, and ultimately the EUCS if it is finalized with similar discriminatory ownership requirements.

If not addressed before finalized, a discriminatory EUCS also threatens to inhibit robust transatlantic cooperation and collaboration in strategic emerging technologies such as artificial intelligence, machine learning, quantum computing, and biotechnology, including at the NATO level among allies.

We appreciate the attention given to these concerns and recommendations, and we support your work to further strengthen the success of the transatlantic partnership.

Sincerely,

ACT | The App Association
BSA | The Software Alliance
Computer & Communications Industry Association (CCIA)
Coalition of Services Industries
The Global Data Alliance
INCOMPAS
National Foreign Trade Council (NFTC)
Software & Information Industry Association (SIIA)
U.S. Chamber of Commerce
U.S. Council for International Business (USCIB)