U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

December 2022

The European Union’s Proposed Cybersecurity Certification Scheme for Cloud Services (EUCS):

How “Sovereignty” Requirements Undermine Cybersecurity and Harm Transatlantic Ties

What is EUCS?

- EUCS was originally designed as a voluntary cybersecurity certification scheme that companies could use to demonstrate their trustworthiness and the effectiveness of their cybersecurity defenses.
- At the behest of the European Commission and a handful of EU member states—the European Union Agency for Cybersecurity (ENISA) was tasked with adding sovereignty requirements to the proposed certification scheme. As a result, it has moved in a concerning direction, by promoting European “digital sovereignty” to provide new market opportunities for European cloud service providers (CSPs) and, consequently, excluding U.S. and other international companies.
- To be granted the highest level of cybersecurity certification for their operations, CSPs would be subject to new sovereignty requirements that mandate “foreign law immunity.” These requirements go as far as requiring companies to register their global headquarters in Europe to certify. It’s unclear how any company that operates outside of Europe, or that has customers outside of Europe, could possibly comply with such a requirement, whether they are U.S. based, European, or otherwise.
- Rather than adopting a risk-based approach, EUCS does not distinguish between CSPs headquartered in democratic, allied countries and those based in authoritarian nations subject to close state control over their management, data, and supply chains.
- Companies also face EU data localization requirements, along with strict requirements for maintenance and operations of their facilities. Additionally, firms seeking the highest level of cybersecurity certification would need to be based in the EU and have a majority of board members be EU citizens.
- These requirements resemble those included in France’s highly discriminatory national cybersecurity certification scheme, called “SecNumCloud” that explicitly forbid non-European providers from government procurement and other market opportunities.

- While on paper the "immunity" requirements are targeted at the highest level of certification—which is meant to be voluntary—there is a clear threat that those requirements will become the *de facto* standard for scheme compliance, increasingly the baseline in European legislation to demonstrate compliance with the law. This may ultimately lead to the very real threat of practically excluding American and other international cloud providers from the EU market.
- These drastic requirements are sometimes justified by European policymakers based on national security concerns, but national security is outside the EU's competency. Article 4 of the EU treaties clearly states that "national security remains the sole responsibility of each Member State."

Where EUCS stands:

- EU member states remain divided on the introduction of the new sovereignty requirements. An increasing number of countries have expressed frustration with the lack of transparency and political debate on such consequential rules, and instead prefer a risk-based approach to certifying non-EU headquartered cloud providers.
- Process-wise, ENISA is currently in charge of drafting a proposal for the European Commission's consideration. There is consultation with a small number of EU member state experts (through the "European Cybersecurity Certification Group"), but very limited political discussion of or broader visibility into this important process.
- Once ready, ENISA will share its proposal with the European Commission (expected before the end of the year), who in turn will use it as a basis to issue the official EU Cybersecurity Scheme (currently expected before the end of 2023).
- ENISA has been highly reluctant to engage directly with stakeholders, so we have limited visibility into the precise state of the debate or timeline for when the scheme may be finalized.

Our Concerns with EUCS:

- Under the guise of promoting Europe's so-called "digital sovereignty," several proposed requirements (e.g. only certifying companies with a global headquarters in the EU) are **politically motivated** rather than based on sound technical standards, core cybersecurity principles, and best practices. They are designed to siphon away business opportunities from U.S. and other international companies to benefit European champions. Barring U.S. CSPs from key sectors in the European economy would have cascading negative impacts on the firms and consumers who rely on their state-of-the-art technologies.
- Ironically, **European competitiveness and cybersecurity would be considerably compromised** if these proposals are adopted. Foreign CSPs unable to earn the "high" level of certification would be ineligible for numerous government procurement opportunities and business opportunities with organizations designated as critical infrastructure. Moreover, they would face reputational risks with other potential clients. This would impose significant limitations on both the quantity and quality of vendors available to meet the operational needs of governments, businesses, and customers.

- EUCS would **adversely impact European security and resilience** at a time where we and our partners and allies face unprecedented economic and geopolitical challenges. It is widely understood that cloud computing confers significant security benefits over on-premises infrastructure, as it simplifies the task of continuously monitoring for threats and vulnerabilities. Global cloud infrastructures provide superior resilience in the event natural disasters or armed conflicts threaten local data facilities or networks. **Data localization requirements not only lead to higher costs for businesses and consumers, they pose significant liabilities from a security and resilience perspective.**
- Several EUCS requirements are **overtly discriminatory in nature**, including: 1) the requirement for companies to have their headquarters based in the EU and 2) to have predominantly EU national board composition. Many CSPs will fail to achieve the "high" level of certification simply due to the location of their headquarters or ownership structure. In addition to being blatantly targeted at successful U.S.-headquartered companies, these requirements are a clear violation of EU trade obligations under the WTO Government Procurement Agreement. If the scheme becomes a way to certify compliance with the EU's new and upcoming legal requirements, the impact of EUCS could be as severe as a *de facto* market access barrier.

Growing Opposition to EUCS:

- Denmark, Estonia, Greece, Ireland, Lithuania, Poland, Sweden, and the Netherlands all issued a joint non-paper expressing concerns with the political elements of EUCS. They have called for the issue to be discussed at the Council level as a political matter rather than a regulatory issue to be decided at ENISA alone. The letter further calls for the certification scheme to remove nationality requirements, given concerns about potential retaliation from the U.S. and other trading partners.
- Germany has called for future decisions to be made by ministers rather than regulators and for additional transparency about the process.
- German business organization BDI published a position paper in June 2022 acknowledging the political and economic issues created by the inclusion of so-called immunity requirements in EUCS. Such requirements would prevent major German and other European firms from scaling their businesses or operating outside of the EU to ensure such "immunity" from non-EU law.
- Fellow trade associations AmCham EU, BSA, CCIA Europe, and ITI released a joint statement in June 2022 outlining their concerns about using EUCS as a tool to promote digital sovereignty.

Our Recommendations:

- **Limit the scope and facilitate alignment with internationally recognized cybersecurity standards** – Although we support EU cybersecurity certification schemes as a useful tool for harmonization and promoting enhanced security, policy discussions on cloud services should be limited to the technical standards required for CSPs to operate in the EU and based on core internationally recognized cybersecurity standards. Politically motivated considerations such as promoting digital sovereignty should be left out of such decisions.
- **Ensure a transparent process** – A political discussion among ministers—up to and including at the head of government level at the European Council—is clearly warranted, given the significant implications for the European economy and EU relations with critical partners, including the United States.
- **Omit discriminatory policies** – Discriminatory factors such as the location of a company's HQ or the nationalities represented on its board should not be used as a proxy for trustworthiness. Instead, the EU should prioritize a risk-based approach that considers company practices and the requirements that may arise for companies headquartered in authoritarian countries.
- **Remain voluntary** – Companies should maintain the ability to choose if they wish to become EUCS certified or not, rather than being forced to meet a mandatory application of EUCS. The European Commission in its 2023 assessment of the efficiency and use of European cybersecurity certification schemes must engage in an open, transparent, and inclusive consultation process with industry.
- **Include all stakeholder groups in discussions** – All relevant stakeholder groups, including private industry, should be involved in discussions on EUCS to ensure that updates are feasible and actually enhance EU cybersecurity. This process should include a thorough economic impact assessment of how the system would be affected if these problematic sovereignty requirements are ultimately adopted, including taking into account the existence and implementation of third-country law.

Myth: The U.S. Takes the Same Approach – False!

- It's important to clarify how the EUCS proposal differs greatly from the U.S. Federal Risk and Authorization Management (FedRAMP) system. Having a U.S. headquarters is not required to be certified. There are 20 European and other international companies are already certified at the highest level under the U.S. system, including SAP and Software AG (Germany), Enel X (Italy), Copado (Spain), Ipsos (France), Wolters Kluwer (Netherlands) and around a dozen others. This is easily verifiable on the FedRAMP website.
- Moreover, FedRAMP does not dictate domestic ownership, management, or immunity from non-U.S. laws as prerequisites to compete for cloud computing contracts. If the EU were to ultimately exclude majority foreign-owned cloud providers, there would be significant pressure on FedRAMP to retaliate. This is an outcome we should endeavor to avoid.

Conclusion:

- The U.S. Chamber of Commerce and our members have serious concerns about the EU cybersecurity certification scheme as currently considered. It is especially worrying to see these developments in the context of the recently agreed U.S.-EU Data Privacy Framework and the ongoing progress being made under the auspices of the Trade and Technology Council. While we should be making significant strides forward in concert with our European partners, the EUCS project and these proposed "sovereignty" requirements threaten to seriously undermine the trust we've rebuilt between us in recent years.
- We look forward to future engagement with the U.S. government to push back against these discriminatory new requirements to ensure that the European market remains open to competition and that our allies' cybersecurity remains strong.

Additional Background:

- Title III of the Cybersecurity Act (Regulation (EU) 2019/881) establishes a voluntary cybersecurity certification framework for products and services. With a view toward reducing market fragmentation within the internal market, the law tasks the European Agency for Cybersecurity (ENISA) with promulgating voluntary cybersecurity certification schemes for a variety of products and services with security measures based on three risk-based criteria (basic, substantial, and high).
- While the law prevents Member States from instituting national cybersecurity certification schemes that would be covered by the EU level scheme, it does preserve the ability of Member States to adopt or maintain national cybersecurity certification schemes for **national security purposes** (recital 94). This is not surprising, as national security falls outside of the EU's competence to regulate.
- ENISA was requested to prepare EU Cybersecurity Certification Schemes for industrial internet of things (e.g., ICS, SCADA, iIoT), 5G ICT, and cloud services.
- The regulation stipulates that in the preparation of candidate schemes, an open, transparent, and inclusive consultation process must be followed. It specifies a consultive role for the Stakeholder Cybersecurity Certification Group. Article 51 of Title III of the regulation specifically stipulates the security measures that should be achieved, as applicable. These include technical data access controls based on international recognized standards.

The Next Frontier: Space-based Connectivity

Even as the EUCS process continues to move forward, the EU has proposed sweeping, onerous sovereignty requirements for its forthcoming space-based secure communications system. As currently drafted, U.S. and other international companies would not be able to compete for or participate in any related projects, even as a supplier or subcontractor.

The rules are very clear:

> To preserve the EU essential security interest and in particular the security, integrity and resilience of the secure connectivity system, the participants in consortia bidding in a procurement procedure must fulfil the following cumulative criteria:
>
> (i) the entity including its executive management structures are established in one of the EU Member States
> (ii) the entity commits to carry out all relevant activities in one or more of the EU Member States, and
> (iii) the entity is not subject to control by third country or third country entity.
>
> These criteria apply to the concessionaire(s), primes, and suppliers of critical technologies, goods, and services.

This is another area where the U.S. government should vigorously insist on non-discrimination. Space-based connectivity is a public good and economic opportunity that would benefit greatly from increased transatlantic coordination. Further transatlantic divides will drive up costs, reduce efficiencies, and limit our ability to compete with non-market economies in an area that is critical to both economic and national security.

For more information:

- **Vincent M. Voci**, Vice President, Cyber Policy and Operations, Cyber, Space, and National Security Policy Division, U.S. Chamber of Commerce. E-mail: vvoci@uschamber.com
- **Garrett Workman**, Executive Director, Europe, International Division. U.S. Chamber of Commerce. E-mail: gworkman@uschamber.com
- **Danielle Muñoz**, Policy and Program Manager, Center for Global Regulator Cooperation, U.S. Chamber of Commerce. E-mail: dmunoz@uschamber.com