Oceans Apart: The EU and US Cybersecurity Certification Standards for Cloud Services

By Kenneth Propp on June 27, 2023

Blogpost 28/2023

The leaked May 2023 **draft** of the EU's Proposed Cybersecurity Certification Scheme for Cloud Services (EUCS) has caused a stir due to its continued inclusion of strong digital sovereignty requirements. The stated goal of the EUCS is to enable cloud service providers (CSPs) to "**demonstrate their trustworthiness and the effectiveness of their cybersecurity defenses**" to European governments and businesses. EUCS, however, threatens to impose data localization requirements on any CSP aiming to qualify for a high level of cybersecurity certification within the European Union. It also effectively would exclude CSPs headquartered outside the EU from seeking "**the *highest* level of … certification**" on the grounds that such CSPs would not be immune from foreign law. The immunity requirement demands that such CSPs "are operated only by companies based in the EU" with their "registered head office and global headquarters … in a Member State."

A working group of the European Agency for Cybersecurity (ENISA), the body charged with drafting EUCS, discussed the latest (now-leaked) EUCS proposal on 26 May 2023. The European Commission strongly defended the proposal, but according to observers several EU member states, led by the Netherlands, resisted the sovereignty requirements, and asked for an impact assessment. France reportedly preferred the **previous proposal**, while Germany, a pivotal player, maintained an ambiguous silence. As a next step, member states will submit written comments by the end of June 2023, including on the important question of the costs of compliance with the requirements envisaged for high level cybersecurity certification.

Technology trade associations from the United States, Latin America, and Japan have **reacted** with disappointment to this latest ENISA proposal, which appears largely to maintain the restrictive provisions of its earlier draft. U.S. trade groups followed up with a letter to the Departments of Commerce and State and the Office of the U.S. Trade Representative calling for the subject to be raised in ministerial-level conversations during the May 30-31 EU-U.S. Trade and Technology Council meeting in Sweden. Senior U.S. officials reportedly expressed concern about EUCS during the meeting.

Some in Europe have defended the proposed EUCS system by claiming that it is comparable to the U.S. Federal Risk and Authorization Management Program (**FedRAMP**), which "provide[s] … a **risk-based approach** for the adoption and use of cloud services" by the U.S. federal government. However, FedRAMP's overarching security focus, risk-based approach, and general openness toward foreign CSPs, stands in stark contrast to the digital sovereignty and industrial policy focus of EUCS. This article undertakes to dispel the notion that EUCS and FedRAMP are similar programs. It begins with an explanation and comparison of EUCS and FedRAMP and then proceeds to discuss the costs and the potential impacts of EUCS.

EUCS

EUCS is conceived as a harmonized EU cybersecurity standard to help CSPs demonstrate their cybersecurity competence and to decrease security compliance fragmentation across Europe. It is an integral part of the **European Commission's broader strategy** to "enable access to secure, sustainable, and interoperable cloud infrastructures and services for European businesses." Originally created by an *ad hoc* working group within ENISA, a technical body, EUCS took on a political character when ENISA was tasked by "**the European Commission … with adding sovereignty requirements to**" the scheme.

This focus on digital sovereignty is guided **by two related goals**. First, the EU aims to define its own rules in the technology area, rather than remain dependent upon foreign—especially American—technology companies and to "achieve strategic autonomy in the digital sphere and boost European competitiveness in tech." In addition, Brussels seeks to "leverage its tools and regulatory powers to … shape global rules."

The leaked latest version of EUCS draft would impose not only traditional security controls for cloud and virtual environments (e.g., network security, storage, and encryption), but also strict digital sovereignty mandates. This latest draft divides the "high" assurance level into two cloud service evaluation levels (CS-ELs): CS-EL3 ("Level 3") and CS-EL4 ("Level 4"), both of which are "intended to minimize the risk of state-of-the-art cyberattacks."

Level 3 is "suitable for cloud services that are designed to meet specific (exceeding level 'substantial') security requirements for mission-critical data and systems." Level 4 is intended for "data of particular sensitivity that would present risks to society if breached." For example, Level 4 would apply to data "related to secrets protected by law," such as those related to government deliberations, national defense and security, foreign policy, and judicial proceedings. Level 4 would likewise apply to "the protection of privacy, to medical secrecy, and to trade secrets, which includes…information on commercial or industrial strategies…necessary for the accomplishment of essential State functions" like the safeguarding of national security, public order, and human health and life.

To qualify for CS-EL3, a CSP must—at minimum—offer "at least one [contractual] option in which all [data storage and processing] locations are within the EU." The CS-EL4 requirements are even stricter. To achieve this highest certification level: (i) with limited exception, all such processing and storage locations must be within the EU and (ii) a CSP's "registered head office and global headquarters" must be in a Member State. CSPs applying for CS-EL4 certification further cannot be under the "effective control" of a non-EU entity.

The draft EUCS also stipulates that both categories of "high" level cloud service contracts must be governed exclusively by the law of an EU member state and not that of a third country. Insisting that its cloud service providers be "immune" from foreign law is part of a larger European effort to escape the long arm of U.S. national security surveillance and law enforcement authorities, it has been **noted**. The effectiveness of such immunity, however, is far from clear. U.S.-based companies cannot exempt themselves from the reach of these U.S. laws, but neither can any foreign company with at least "**minimum contacts**" with the United States. Indeed, one French cloud company (OVH), certified

under the French version of cloud cybersecurity standards, has explicitly **conceded** that its U.S. affiliate "will comply with lawful requests from public authorities . . . [including] [u]nder the CLOUD Act, that could include data stored *outside* of the United States." Having business contacts with the United States is especially likely to occur for any EU-based cloud service operating at a sufficiently large scale and sophistication to meet the "high" assurance level as defined by EUCS.

These proposed EU-level sovereignty requirements are modelled on France's now-mandatory **SecNumCloud** certification program, which launched in 2016. As explained **here**, the French program requires that CSPs "be 'immune to any extra-EU regulation'" (i.e., not be subject to the laws of a non-EU jurisdiction), "commit to storing and processing data within the European Union," and administer and supervise their "services within the EU." No non-French CSPs have met these requirements. While EUCS, like SecNumCloud when first introduced, is currently voluntary, there is a strong possibility that it "**could be made mandatory**" under the NIS2 Directive, potentially leading to similar outcomes throughout Europe.

Including majority domestic local ownership requirements may also be inconsistent with international trade obligations. Two existing sets of rules, both promulgated by the World Trade Organization (WTO), govern cross-border provision of services: the **Government Procurement Agreement** (GPA), which addresses government acquisition specifically, and the **General Agreement on Trade in Services** (GATS), which applies more broadly.

The GPA requires that any state party treat foreign companies supplying cloud services on a cross-border basis to government entities no less favorably than locally-established suppliers (the principle of 'national treatment'). GATS contains similar national treatment commitments, as well as a right to market access in sectors including computer and related services. In their letter to U.S. government leaders, the technology trade associations expressed the view that the EUCS is "almost certainly inconsistent" with these national treatment obligations. On 5 June 2023, U.S. Ambassador to the World Trade Organization Maria Pagan **called out** EUCS in remarks during a meeting reviewing the EU's trade policies.

Both agreements allow exceptions for national security, privacy, and other public policy interests. The European Commission may have designed the latest iteration of EUCS to arguably fit within such exceptions, by liberally referring not only to national security but also to public order, public safety, public health, and the protection of trade secrets. There is little WTO precedent in applying the GPA and GATS to cloud services, so the outcome of any potential dispute settlement proceeding would be highly uncertain.

FedRAMP

ENISA's sovereignty mandates are quite unlike the general certification scheme laid out by the U.S. FedRAMP program, through which **both US and foreign companies may become certified** cloud providers for the U.S. federal government. As set forth in the Office of Management and Budget's (OMB) 2011 memorandum (hereinafter OMB Memo) establishing the program, FedRAMP's primary goal is to develop "trusted relationships between Executive departments and agencies" and CSPs.

FedRAMP created two pathways by which U.S. and non-U.S. CSPs can become certified to participate in U.S. federal cloud-related contracts. One option is for a CSP to go through the '**agency process**,' in which individual federal agencies "work directly with [CSPs] for authorization at any time," and gain accreditation by a specific federal agency assessing the CSP against existing security control frameworks published by the National Institute of Standards and Technology (NIST). In the alternative, CSPs may seek certification via the Joint Authorization Board (the '**JAB process**'). The JAB, also known as the FedRAMP Board, is the interagency governing body for FedRAMP and includes representatives from the U.S. Department of Defense, Department of Homeland Security, and General Services Administration. Under either process for achieving FedRAMP accreditation, a CSP must undergo security and readiness assessments and work with a third-party auditor to certify in conformity with NIST controls.

To that end, FedRAMP employs a "risk-based approach", whereby information managed by CSPs is categorized "**based on the potential impact that certain events would have on an organization's ability to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals.**" In part because of its risk-based approach, "FedRAMP does not provide or specify **data location requirements**" for low or moderate risk systems. Rather it only specifies "data location requirements [for CSP systems] in the" high risk category, which includes "law enforcement and emergency services systems, financial systems, health systems, and any other systems where loss of confidentiality, integrity, or availability could … have severe or catastrophic adverse effect[s]." These security requirements are set through a broader NIST process, which involves extensive engagement with external stakeholders.

The FedRAMP risk-based approach differs from EUCS in three ways. First, the relevant risk under FedRAMP is based on technical and administrative cybersecurity factors, rather than on sovereignty and the nationality of the CSP. **Indeed**, "the list of FedRAMP-certified products contains the cloud service offerings of many non-U.S.-based firms, including several at the high level."

Second, the "high" impact category in FedRAMP applies to a small minority of government systems, in contrast to the possibility that the EUCS "high" level will apply far more broadly. Under FedRAMP, CSPs are divided into low, moderate, and high impact categories depending on the nature of the adverse effects such events would have in the event they disrupted their services. Most (**nearly 80%)** CSP applications that receive FedRAMP authorization are deemed moderate impact systems, while only a handful are low or high. For example, critical government services such as national archives and small business aid programs run at the moderate level.

Following this risk-based approach enables FedRAMP to formulate minimum security requirements for CSPs falling within each category rather than to impose location requirements on potentially a large portion of systems. In other words, for the over 80% of CSP systems not deemed high risk, FedRAMP does not require that data be stored in the United States. This differs from EUCS, which would impose strict localization and immunity mandates for CSPs handling data related to a much broader set of public purposes.

Third, FedRAMP applies only to contracts for government services. By contrast, SecNumCloud already **applies** to a wide variety of commercial services deemed "vital" or "essential." EUCS would have a similarly broad effect on the many critical infrastructure services provided by the **private sector**, since "the high assurance level is expected to

become mandatory for the essential and important services listed under the [Network and Information Services 2] Directive."

FedRAMP's scheme is separate from other U.S. government efforts to protect against risks posed by digital adversaries like Russia and China. Mechanisms geared toward curbing threats from adversaries include government contracting standards for vendors holding **Controlled Unclassified Information** or more highly classified data; federal agency (e.g., Department of Defense) acquisition standards; and review by the Committee on Foreign Investment in the United States (CFIUS) of proposed foreign investment that could affect national security. One salient example of these non-FedRAMP measures are the **federal acquisition** regulations banning the purchase and use of telecommunication equipment and services from Huawei and ZTE.

Unlike EUCS' potentially broad exclusion of non-EU CSPs from many public contracts, the U.S.' more nuanced system encourages the participation of secure allies as well as U.S. entities, while at the same time blocking threats from adversaries. The EU could achieve a similar outcome by looking at **alternatives proposed by Member States** in a paper earlier this year, including one for assessing trustworthiness of non-EU CSPs. Germany's IT Security Law 2.0, which looks at NATO allies as trustworthy, and the risk profiles of the 5G toolbox are referenced as potential models for assessing trustworthiness.

The Costs of Digital Sovereignty for Cybersecurity

The European Commission aims to achieve significant goals, which include increasing the market for European CSPs, improving cybersecurity across the European continent, creating uniformity among compliance and certification programs, and blocking foreign jurisdictions from accessing European cloud data. However, EUCS' data sovereignty dimensions significantly undermine its ambitions.

Scholars have pointed out that "European competitiveness and cybersecurity would be considerably compromised if" EUCS is adopted. Because many "[f]oreign CSPs [would be] unable to earn the 'high' and 'highest' levels of certification," they would "be ineligible for numerous government procurement opportunities and business opportunities with organizations designated as critical infrastructure." As a result, European governments and highly important business entities could be forced to use smaller and less-sophisticated European CSPs that are less capable of supporting their cybersecurity needs. Indeed, it can take years for stable enterprise architecture to develop, as noted by the **European Association of CCP Clearing Houses**, which has expressed concern about EUCS' potential to limit financial clearing houses' ability to access best-in-class cybersecurity technology only available via non-EU providers.

In addition, detailed studies, **here** and **here**, have concluded that "data localization often creates obstacles to integrated management of cybersecurity risks," while at the same time reducing "the effectiveness of purchasing cybersecurity-related services." For instance, localization can lead to increased complexity for government and business entities as they must manage their cyber and cloud needs without access to a global network of service providers and support. Localization also hinders CSPs' cross-border sharing of information to address security issues, **including for standard cybersecurity tasks** such as penetration testing and prevention against escalation of privileges.

Conclusion

Thus, while EUCS may—over time—spur the growth of European CSPs and increase uniformity among cybersecurity standards across the continent, the imposition of digital sovereignty requirements (localization and foreign law immunity) would impose substantial costs on CSP users in Europe, at least in the medium-term. At a minimum, such an approach should be subjected to a public consultation process and full impact assessment that would fully explore the potential costs, as advocated by several member states, including the Netherlands.

The EU also should consider the broader geo-political context. Brussels appears to be overlooking the crucial role that U.S. cloud service providers have played in **enabling Ukraine rapidly to shift government services** to secure cloud platforms. In addition, **the EU** has failed to distinguish between risks of government access from rule of law countries like the United States and those emanating from authoritarian states with sweeping national security laws. Conflating the two appears at odds with the direction that the EU and the United States are taking in the **Trade Technology Council** and the new Data Privacy Framework, which instead focus on building transatlantic economic security. Trustworthiness in cloud cybersecurity must begin with a clear sense of who your allies – and adversaries – are.

The authors would like to thank Amy Mushawar of Alston & Bird LLP for her contributions to an earlier version of this research.