ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

Europe's Cloud Security Regime Should Focus on Technology, Not Nationality

NIGEL CORY I MARCH 2023

The EU's new cloud cybersecurity regime should focus on good security practices, as the U.S. FedRAMP regime does. Emulating China's protectionist focus on firm nationality is a bad security practice that weakens transatlantic influence over cybersecurity issues globally.

KEY TAKEAWAYS

- Like China, some European Union (EU) countries want to misuse cloud cybersecurity rules for the protectionist purpose of replacing leading U.S. cloud firms such as AWS and Google with local champions.
- The proposed European Cybersecurity Certification Scheme for Cloud Services (EUCS) follows China's approach of making local firm ownership and control the defining factors in ascertaining whether a cloud service provider can be trusted.
- The EUCS differs from the U.S. Federal Risk and Authorization Management Program (FedRAMP) in several respects: It focuses on firm ownership, uses closed and politicized technical standards, and assesses services for the private sector, not just government.
- Protectionist proponents of the EUCS (namely France) want it all: local cloud firms, not American ones, but with all the cybersecurity assistance they can get from the U.S. government and the same U.S. cloud firms they want to exclude from their markets.
- A protectionist EUCS would undermine transatlantic digital trade by making the new Transatlantic Data Privacy Framework irrelevant, since U.S. firms would be precluded from managing a considerable amount of EU data, never mind transferring it overseas.
- The EU and its member states should remove the protectionist restrictions from the EUCS, focus on the actual technicalities of cybersecurity, and work with the United States on global cybersecurity issues through the EU-U.S. Trade and Technology Council.

CONTENTS

Key Takeaways 1

Introduction 3

Stopping Data Flows and Cloud Market Access Undermines European, Transatlantic, and Global Cybersecurity 5

Explaining the U.S. FedRAMP System for Cloud Cybersecurity 6

How America's FedRAMP Differs From Europe's "Sovereignty"-Based Approach to Cybersecurity 8

- FedRAMP Is Open to Firms From Around the World 8
- FedRAMP Focuses on Cybersecurity Practices, Not Firm Structure and Ownership 8
- Data Localization Is a Misguided but Thankfully Minor Part of FedRAMP, Yet It Is Central to SecNumCloud and the EUCS Proposal 9
- FedRAMP Is Only Used by Federal Government Agencies and Does Not Impact U.S. Critical Infrastructure or the Broader Commercial Cloud Market 9
- NIST Cybersecurity Standards Are Open, Transparent, and Technically Focused—ENISA and EUCS Processes and Standards Are Not 10

Recommendations 11

- Use Standards "Crosswalks" to Build Transatlantic Cybersecurity Cooperation 12
- Negotiate a Transatlantic Agreement on Law Enforcement Access to Data 13
- Allow the Mutual Recognition of U.S./EU Cybersecurity Certification and Auditing Programs 14

Conclusion 14

Endnotes 15

INTRODUCTION

Like China, some European Union (EU) countries want to misuse cloud cybersecurity rules to replace leading U.S. cloud firms such as AWS, Google, and Microsoft with local ones—in other words, enacting digital protectionism.[1] The European Cybersecurity Certification Scheme for Cloud Services' (EUCS) is the vehicle by which the EU wants to sneak this protectionist scheme into operation. At first glance, the EUCS is similar to what the U.S. Federal Risk and Authorization Management Program (FedRAMP) does for the U.S. federal government: provides a harmonized approach to cloud cybersecurity certifications to both ensure a better overall level of protection and reduce the cost and complexity for firms and government agencies contracting cloud services. However, unlike FedRAMP, the EUCS follows China's approach in making local firm ownership and control—rather than the use of best-in-class cybersecurity practices—the defining factors in ascertaining whether a cloud service provider can be deemed "trusted" and allowed to operate in the local market. This would have a major impact on transatlantic digital trade. By excluding U.S. cloud firms, the EUCS would make the new Transatlantic Data Privacy Framework (TDPF) irrelevant, as U.S. firms would be precluded from managing a considerable amount of data in the EU, never mind transfer it overseas—while abiding with the EU's General Data Protection Regulation (GDPR). The EU and its member states should remove these protectionist restrictions, focus on the actual technicalities of cybersecurity, and work with the United States on global cybersecurity issues at the EU-U.S. Trade and Technology Council (TTC). If they do not, the Biden administration should retaliate.

Perhaps not surprisingly, France is leading the push to use the EUCS for digital protectionism. This follows French efforts to replace American tech firms with local ones in search engines, online short-term housing rentals, and cloud services.[2] The EUCS is based on sovereignty requirements included in France's national "SecNumCloud" cybersecurity regime, which incorporates foreign ownership and management restrictions, forced local data storage requirements for personal and nonpersonal data, and local staff requirements. Two earlier reports from the Information Technology and Innovation Foundation (ITIF) analyze these provisions, explaining how they breach French and EU trade law commitments under the World Trade Organization's (WTO's) Government Procurement Agreement and the General Agreement on Trade in Services.[3] In forcing foreign firms to set up minority-owned joint ventures to be deemed "trusted," the EUCS proposal unfortunately copies China's approach.[4]

U.S. FedRAMP differs from the EUCS in three key ways: FedRAMP focuses on cybersecurity technicalities, not firm ownership; FedRAMP is only used by the federal government, while the EUCS may be used more broadly in the economy; and FedRAMP is based on open and transparent standards, EUCS is not.

Ultimately, France wants it all and has the gall to push for it: It wants local cloud firms, not American ones, plus all the cybersecurity assistance it can get from the U.S. government and those same U.S. cloud firms. French policymakers use the hypothetical risk that U.S. law enforcement agencies have extraterritorial access to data under U.S. law (namely, the Clarifying Lawful Overseas Use of Data Act or CLOUD Act) to target U.S. cloud firms.[5] Even Guillaume Poupard, the outgoing director of France's cybersecurity agency, admitted that a 100 percent French "sovereign" cloud is unrealistic.[6] After years of leading the attack against U.S. cloud

providers, Poupard recently told the French Senate that French customers will need to continue to rely on partnerships with U.S. providers.[7] Yet, this won't stop France's ongoing effort to attack U.S. tech firms. However, it should hopefully give pause to other EU policymakers about the cybersecurity, trade, and economic risks of blindly following France's lead.

In contrast, European policymakers should follow America's FedRAMP lead in implementing the EUCS. FedRAMP differs from SecNumCloud and EUCS sovereignty requirements in three key ways. First, FedRAMP focuses on the technicalities of cloud cybersecurity and not the ownership of a firm; many foreign firms are certified under FedRAMP. Second, FedRAMP only applies to the cloud services used by U.S. federal government agencies, not the broader market.[8] SecNumCloud and the EUCS could potentially apply to a broad part of the EU economy. Third, the U.S National Institute of Standards and Technology (NIST) sets the technical cybersecurity standards used by FedRAMP in an open and transparent manner, unlike the closed and politicized approach taken by the European Union Agency for Cybersecurity (ENISA) in developing the standards for the EUCS.

Some European officials have justified EUCS sovereignty requirements, in part because they mistakenly think they are like provisions in FedRAMP—which is false. This briefing details these differences and provides ideas for a constructive transatlantic agenda on cybersecurity. It explains what FedRAMP is—and, most importantly, isn't—in comparison with SecNumCloud, and how it's critically important that Europe remove the restrictive and misguided sovereignty requirements in the EUCS proposal. The report then outlines a constructive agenda for transatlantic cooperation on cybersecurity.

A summary of the recommendations:

- France, Germany, Italy, and their other EU member states should remove the sovereignty provisions in their SecNumCloud-inspired proposal for the EUCS (and in France's own SecNumCloud). The United States should ramp up engagement with Germany and the European Commission at TTC to ensure this happens.
- If Europe fails to remove these restrictions, the United States should reevaluate cybersecurity cooperation and information sharing with the EU and its member states and develop and initiate retaliatory measures.
- The EU and United States should use TTC to improve cybersecurity cooperation via standards "crosswalks" to identify commonalities, differences, and potential future work to ensure compatibility in the development and use of cybersecurity standards in their respective systems.
- The United States and EU should provide high-level attention and support to newly restarted efforts on an e-evidence/CLOUD Act agreement, just as they did with the forthcoming TDPF.
- The United States and EU should work toward the mutual recognition of U.S./EU Cybersecurity certification and auditing programs.

STOPPING DATA FLOWS AND CLOUD MARKET ACCESS UNDERMINES EUROPEAN, TRANSATLANTIC, AND GLOBAL CYBERSECURITY

Cybersecurity constitutes a growing part of foreign, trade, and national security policy. However, if leading U.S. cloud providers are not "trusted" in Europe, they can't share information and take coordinated action as part of the public-private collaboration needed to combat global cybersecurity incidents.[9] The public-private collaboration and information sharing at the heart of international cooperation are getting harder, with growing market access barriers and data transfer restrictions around the world.[10]

Government cybersecurity agencies already find it challenging to have collaborative—and not confrontational—relationships with cloud firms.[11] Public-private cybersecurity information sharing can be difficult in many countries, as firms need legal protections for the confidentiality of the information they share (given potential legal and regulatory implications). Adding data localization and local control and ownership barriers would make public-private collaboration even more difficult, if not impossible.[12]

For example, in the first systemic analysis of data localization's impact on cybersecurity, Peter Swire and DeBrae Kennedy-Mayo have shown how it seriously undermines good cybersecurity.[13] Localization prevents the sharing of cybersecurity-related information. It also undermines 13 of the 14 controls in one of the main international standards for information and cybersecurity (ISO/IEC 27002).[14] Localization also prevents local organizations from accessing best-in-class cybersecurity services.

U.S. cloud firms need market access, and seamless data flows, to both share information and take preventative and remedial action in the event of cyberattacks. They also need to transfer data to learn from their global operations to better detect and respond to cyberthreats in Europe. Under the EUCS, cloud providers would no longer be able to seamlessly map global threat patterns against domestic ones or trace signs of malicious activity from global networks onto domestic ones.

If Europe does not trust U.S. cloud firms at home, how can the EU and United States make the case to governments in third-country markets to trust them as part of new transatlantic efforts to support their firms in building digital infrastructure in developing countries?

For example, in 2022, Google Cloud and other cloud firms defended themselves and their customers from the largest distributed denial-of-service attack on record—at 46 million requests per second—in part because they were able to identify it early on, as there were anomalous spikes in activity from IP addresses in four countries simultaneously: Brazil, India, Indonesia, and Russia.[15] If Google and other global cloud providers lose the ability to collect and share security telemetry from around the world, it's going to be far more challenging to respond to cyberthreats and attacks in Europe and elsewhere around the world.

Sovereignty requirements would also make it harder, if not impossible, for U.S. firms to take preventative action to protect European customers and cybersecurity agencies in the run-up to a cyberattack. It would also be harder for cloud providers to ensure all service vulnerabilities are patched if their IT infrastructure is fragmented or disconnected from the global cloud. Joint

incident analysis between government agencies and firms would also be harder, if not impossible, if U.S. and other foreign firms were excluded from Europe's market.

European cloud sovereignty requirements would preclude transatlantic and global cybersecurity cooperation before it even starts. In 2022, the United States and Europe launched their first joint effort to fund their firms inbuilding secure critical and digital infrastructure in developing countries (as an alternative to Chinese firms).[16] However, it's hard to see how this could continue if Europe enacts sovereignty requirements. If Europe does not trust U.S. cloud firms at home, how can they make the case to governments in third-country markets to trust them?

EXPLAINING THE U.S. FEDRAMP SYSTEM FOR CLOUD CYBERSECURITY

The U.S. FedRAMP program provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud services used by U.S. federal government agencies.[17] As ITIF argued in "Reforming FedRAMP: A Guide to Improving the Federal Procurement and Risk Management of Cloud Services," the time and cost of getting FedRAMP certified could be improved.[18] However, overall, it provides a common, high level of cloud cybersecurity protection instead of each agency designing its own cloud cybersecurity specifications for contracts.

FedRAMP is specifically tailored to risk. It specifies controls according to three impact levels: low, medium, and high.[19] NIST sets the technical requirements for each level.[20] The higher the impact level, the more baseline controls required: 123 controls for low-impact systems, 325 for moderate-impact systems, and 421 for high-impact systems. Low-impact risks include data intended for public use, so any loss of data wouldn't compromise an agency's mission, safety, finances, or reputation. Moderate-impact risks include data that's not available to the public, such as personally identifiable information, such that a breach can have a serious impact on an agency's operations. Most U.S. federal government agencies operate at this moderate-impact level (in 2017, nearly 80 percent of FedRAMP applications were for this level) given their use of "controlled, unclassified information."[21]

High-impact risks include sensitive (but unclassified) federal information, such as law enforcement, emergency services, and health care data, so breaches to government systems containing this data would be highly damaging. In 2017, the Department of Defense (DOD) accounted for 33 percent of high-baseline use in the U.S. government, followed by the departments of Veterans Affairs (16 percent), Homeland Security (13 percent), and Justice (10 percent).[22]

FedRAMP assessments are focused on specific cloud services. FedRAMP does not assess and authorize firms overall, but rather their "cloud service offering" (CSO) at specific impact levels. Each CSO goes through several assessments before approval.[23] Each CSO Readiness Assessment Report (RAR) is assessed within an "authorization boundary," which is essentially a review of the internal services, components, and other devices along with connections to external services and systems.[24] If needed, the RAR will detail what changes the firm will need to make (and be confirmed) before its CSO is considered ready.

FedRAMP certification is not a one-and-done assessment.[25] Once a CSO is in the FedRAMP marketplace, it will need to go through annual assessments. Also, monthly monitoring details need to be submitted to the Joint Authorization Board (JAB), which is the decision-making body

for FedRAMP.[26] For example, for moderate-/high-impact services, cloud service providers must mitigate all discovered high-risk vulnerabilities within 30 days, mitigate moderate-vulnerability risks in 90 days, and mitigate low-vulnerability risks in 180 days.

FedRAMP uses expert third-party assessment organizations (PAOs) to assess CSOs. PAOs include specialist IT compliance, auditing, and advisory firms such as A-Lign, Schellman, Fortreum, Kratos, Lunarline, and dozens of others.[27] PAOs themselves must meet FedRAMP-specific requirements and international best practices, such as the standard ISO/IEC 17020 on requirements for bodies performing conformity assessments.[28] PAOs assesses a CSO's ability to maintain a clearly defined system boundary, ability to describe intra and inter-system dynamics, user and sensitive metadata flow, risks associated with interconnections used to transmit federal or sensitive data, and risks associated with the use of external systems and services that are not FedRAMP authorized, among other issues.

FedRAMP is tailored to risk, using three impact levels: low, medium, and high. In 2017, nearly 80 percent of FedRAMP applications were for the moderate level, given government agencies' use of "controlled, unclassified information."

NIST maintains and updates the guidelines and technical standards at the heart of FedRAMP's assessment framework, especially NIST's "special publications" on system controls and risk management. The current standard is NIST's "Special Publication 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations" series. Within this "800 series" publication are guidelines on many specific issues.[29] NIST continuously updates its guidelines, and then periodically (every five or so years) does a full review and update. For example, NIST is currently revising guidelines as part of its "Revision 5" within an open and transparent process, with opportunities for industry and government feedback, to ensure it accurately reflects best practices.[30]

Data localization is a very small and narrowly tailored part of FedRAMP. FedRAMP does not include misguided data localization requirements, but individual U.S. government agencies can require it as part of a CSO. Only FedRAMP's high-impact services include the option for agencies to require data localization.[31] Only in 2020 did FedRAMP's JAB add data localization as an optional requirement for a FedRAMP high-impact rating to create reciprocity between FedRAMP and DOD's Security Requirements Guide (SRG)—which is DOD's own process for authorizing cloud providers. DOD SRG impact level 4 is very similar to FedRAMP high, except that the former contains a data localization requirement. JAB and the Defense Information Systems Agency negotiated this compromise so that in exchange for JAB adding a data localization option to FedRAMP high, DOD would grant reciprocal authorization at impact level 4 to any CSO authorized at FedRAMP high.

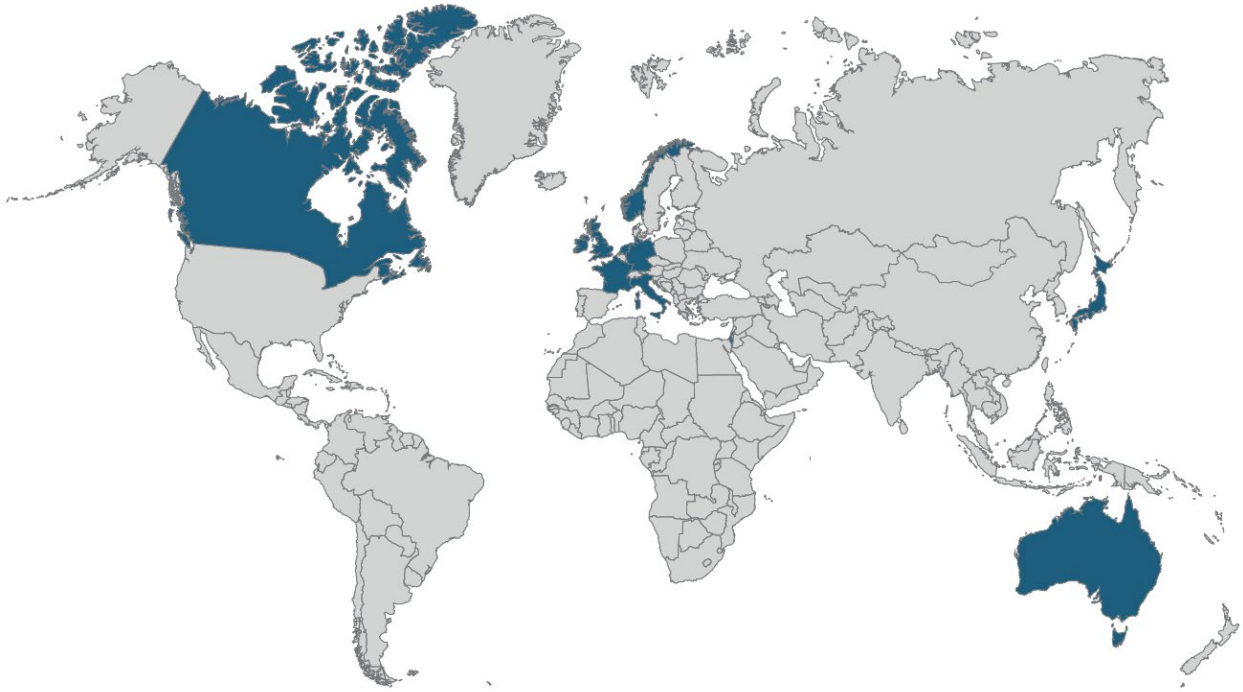
HOW AMERICA'S FEDRAMP DIFFERS FROM EUROPE'S "SOVEREIGNTY"-BASED APPROACH TO CYBERSECURITY

The following sections detail how the U.S. FedRAMP program is fundamentally different from France's SecNumCloud and the EUCS proposal.

FedRAMP Is Open to Firms From Around the World

FedRAMP is open to U.S. and foreign firms (see figure 1). Cloud firms from any country can apply for FedRAMP accreditation; there are no nationality or ownership restrictions. As of November 2022, of the 285 FedRAMP-authorized service offerings and the 78 undergoing review, (at least) 20 companies were either headquartered abroad or U.S. subsidiaries of foreign firms (e.g., Siemens Government Technologies Inc.) that are either FedRAMP authorized or pending authorization. These include Accenture (Ireland), Acendre (Australia), Blackberry (Canada), Canon (Japan), Collabware (Canada), Deloitte (United Kingdom), Enel X (Italy), Evidence Prime (Canada), Ex Libris (Israel), Geotab (Canada), Hootsuite (Canada), Huddle (United Kingdom), Ipsos (France), Itamar Medical (Israel), MicroFocus (United Kingdom), Pexip (Norway), SAP (Germany), Siemens (Germany), Thomson Reuters (Canada), and Wolters Kluwer (Netherlands). Accreditation levels vary; however, Accenture, Collabware, and Siemens, for example, are all authorized at FedRAMP high.

Figure 1: Countries with firms in the process of receiving FedRAMP accreditation



FedRAMP Focuses on Cybersecurity Practices, Not Firm Structure and Ownership

FedRAMP is focused on developing and auditing firms' use of best-in-class cybersecurity practices, not the ownership or control of firms. The best analog for FedRAMP in Europe is Germany's C5 Standard, which is also a purely technical cybersecurity certification regime.[32] In contrast, many SecNumCloud requirements relate to legal aspects, organizational structure, and

investment and ownership—considerations that are unrelated to technical-based certification of cloud services or improving cybersecurity.

Data Localization Is a Misguided but Thankfully Minor Part of FedRAMP, Yet It Is Central to SecNumCloud and the EUCS Proposal

Whether it's in China, France, or the United States, data localization is a misguided policy—even in the case of government data and services. Localization does not improve data privacy or security.[33] For example, the hack of the U.S. Office of Management and Budget—one of the most notorious hacks, given the U.S. government data involved—occurred against data services on-premises in U.S. government agencies.[34] Localization's use in FedRAMP as part of contracts with specific U.S. federal government agencies means it's very narrowly applied. Its use does not impact the broader, and much larger, commercial U.S. cloud services market.

Data localization is bad for cybersecurity, regardless of whether it involves commercial or government data.

The United States' limited use of localization is like Canada's public cloud market, which is also open to foreign firms and products and requires limited local storage for sensitive and classified data (at rest) in Canada. However, Canada still allows data to move (i.e., data in transit), as it recognizes that certain cloud services can be run outside Canada.[35] Both the U.S.'s and Canada's narrow conceptualization and application of localization for sensitive government data and services is far preferred over the broad, vague national security concerns China, France, and others in Europe assert as a rationale for digital protectionism.

FedRAMP Is Only Used by Federal Government Agencies and Does Not Impact U.S. Critical Infrastructure or the Broader Commercial Cloud Market

FedRAMP is a cloud cybersecurity framework specifically for cloud providers that store or process data for the U.S. federal government. It is not required for the broader array of sectors and firms deemed part of critical infrastructure (as in SecNumCloud).[36] The U.S. government's procurement market for cloud services is small relative to the rest of the economy.

In comparison, SecNumCloud and EUCS sovereignty requirements could effectively preclude foreign cloud firms from providing services to government agencies and or competing across a broad swath of the commercial economy. For example, in France, it applies to firms providing services to the government as well as to 600-plus firms that operate "vital" and "essential" services. As Ireland, Sweden, and the Netherlands detailed in a letter outlining their concerns about SecNumCloud, it exerts broad commercial and trade implications.

The EUCS is a work in progress, so its scope is still in flux, but there are several highly problematic proposals under consideration that would substantially expand its scope beyond high-impact workloads affecting classified information and national security to moderate/substantial or low/basic use cases (depending on the tier terminology the EUCS adopts). This would be in addition to covering critical infrastructure, which is a broad part of the economy, including financial services, energy, transportation, utilities, telecommunications, and other sectors. Alternatively, in the best-case scenario, there is also a proposal to narrow the scope

of EUCS so that it is narrower than FedRAMP, applying only to national security or classified workloads.

The EUCS could have a broad impact on the EU's digital economy. Even if it only applies to sensitive and high-impact areas, it's expected that all providers would strive for this high certification because cloud services are usually just one part of a broader ecosystem of providers for government agencies and firms serving vital infrastructure and related sectors. In this way, it will essentially become mandatory to be certified at the highest level.[37]

The EUCS's broad application would also become mandatory in many sectors if it is connected to relevant EU legislation, such as the Network and Information Security (NIS) Directive and the Digital Operational Resilience Act (DORA, which is focused on ICT security for financial firms). Moreover, EUCS sovereignty requirements could conflict with those rules. For example, the Association for Financial Markets in Europe (AFME) points out that DORA allows ICT services to be provided from outside the EU. However, ASME assesses that it's likely cloud providers would need a high-impact certification to serve financial firms (given the sector's likely designation as critical infrastructure), and thus EUCS sovereignty requirements would directly conflict with DORA.[38]

NIST Cybersecurity Standards Are Open, Transparent, and Technically Focused—ENISA and EUCS Processes and Standards Are Not

As detailed in ITIF's report "How the EU Is Using Technology Standards as a Protectionist Tool In Its Quest for Cybersovereignty," NIST cybersecurity standards are developed in an open, transparent, and technically focused manner, such that each provision and control is analyzed, proven, and vetted by cybersecurity and cloud experts from around the world. Most recently, NIST did this as part of a global competition to select the best post-quantum encryption standard.[39] By running an open process, NIST hopes that it will not only lead to the best standards but drive global support for these standards as stakeholders recognize that NIST's approach is the most rigorous. Similarly, NIST runs an open process when it revises and updates the core cybersecurity standards at the heart of FedRAMP.

The EU Agency for Cybersecurity has politicized the process for setting cybersecurity standards, putting sovereignty requirements off-limits from discussions and trying to include them as part of the EUCS implementing act so as to avoid high-level political discussions at the EU.

In contrast, ENISA has been criticized by U.S. and European firms and industry associations, and some EU member states, for lacking transparency and stakeholder engagement in developing technical standards for the EUCS.[40] Industry stakeholders and certain EU member states have been left in the dark on developments and ultimately asked to accept the final version as a fait accompli.[41] While there are several bodies, such as the European Cybersecurity Certification Group, the Stakeholder Cybersecurity Certification Group, and various ad hoc groups of experts that are supposed to advise ENISA on the framework and its technical standards, in practice, these outside stakeholders are relegated, never really consulted, and largely ignored.

For example, ENISA made it clear to the ad hoc working group on cloud services that they were allowed to review, comment, and improve on the "independence from non-EU law" requirements

(Annex J, which is central to the discriminatory sovereignty requirements) in the EUCS proposal, but that they were not to consider whether ENISA should remove or revise these sovereignty requirements. Similarly, ENISA tasked the European standards organizations making the technical standards to work only on the actual technical and organization components related to cybersecurity and not the sovereignty requirements.[42] Instead, these sovereignty "eligibility criteria" will be included as clauses in the implementing act to be assessed by EU member states' national cybersecurity certification authorities. In essence, ENISA is attempting an end-run around higher-level political considerations at the European Commission and an open and transparent debate over technical standards (as required under WTO trade law).

RECOMMENDATIONS

The European Commission and EU member states should remove these protectionist cloud requirements in order to demonstrate that they genuinely want to work with the United States and other likeminded countries on cybersecurity and other digital issues.

The following section includes recommendations for immediate action, followed by medium- and long-term ideas for EU-U.S. cybersecurity cooperation.

Key recommendations:

- **France, Germany, Italy, and other EU member states should remove the sovereignty provisions in their SecNumCloud-inspired proposal for the EUCS (and in France's own SecNumCloud).** Thankfully, some EU member states (e.g., Ireland, Sweden, and the Netherlands) recognize that France's approach via SecNumCloud is not only misguided, costly, and counterproductive, but also an end-run around the legislative process given that SecNumCloud sovereignty requirements have no legal justification under the EU GDPR or any EU cybersecurity law (e.g., the Cybersecurity Act or NIS Directive). These countries, and others, need to do more to ensure the EUCS process focuses on technical cybersecurity issues as opposed to political concepts such as sovereignty.[43]
- **The United States should ramp up engagement with Germany on the issue.** It has supported efforts made by France, Italy, and Spain to support immunity requirements in the EUCS scheme; however, of late, some German policymakers and institutions have realized that this approach is misguided.[44]
- **The United States should use TTC to press against SecNumCloud requirements.** These **requirements** are a clear breach of both EU member state and the EU's commitments at the WTO (as detailed previously) and clearly undermine TTC. Failing the removal of these provisions, the United States should take retaliatory action.[45]

If France, Germany, and the EU fail to remove sovereignty requirements, the United States should do the following:

- **Reevaluate cybersecurity cooperation and information sharing with the EU and its member states.** If Europe wants to go it alone on cybersecurity, then it should be on its own the whole way. It shouldn't be allowed to benefit from broad U.S. government and commercial cybersecurity cooperation while simultaneously targeting the latter via protectionist policies.

- **Develop and initiate retaliatory measures.** At a minimum, if Europe proceeds with the EUCS along these lines, the United States should immediately remove European firms that benefit from FedRAMP. It should also consider how to exclude European firms from forthcoming cybersecurity regulations. The United States Trade Representative's Office should use Section 301's long-overlooked provisions relating to barriers to services trade, such as via licensing, certification, and other restrictions. It should also engage Japan, the United Kingdom, Singapore, and others in a trade dispute against the EU and individual EU member states for breaching the WTO's Agreement on Government Procurement (GPA), General Agreement on Trade in Services (GATS), and Technical Barriers to Trade (TBT) rules.

Use Standards "Crosswalks" to Build Transatlantic Cybersecurity Cooperation

The EU and United States should use TTC to improve cybersecurity cooperation via standards "crosswalks" to identify commonalities, differences, and potential future work to ensure compatibility in the development and use of cybersecurity standards in their respective systems. While harmonized technical standards would be ideal—so that firms could use one standard globally—absent this, standards crosswalks would provide a pragmatic and valuable way to build bridges between their respective regulatory and standards systems. In cases where standards don't yet exist, crosswalks could identify the most promising areas of standards development.

Incidentally, the EU and United States have already proven standards crosswalks are useful, as U.S. and EU government officials and private sector representatives did a crosswalk of the NIST Cybersecurity Framework and the EU's Cybersecurity Act/NIS Directive. Furthermore, the Ministerial Declaration following the Paris-Saclay TTC meeting on artificial intelligence (AI) cooperation provides an opening for a potential crosswalk assessment between the EU's AI Act and NIST's proposed AI Risk Management Framework.

EU-U.S. cybersecurity "crosswalks" could identify commonalities, differences, and potential future work to ensure compatibility in the development and use of cybersecurity standards in their respective systems.

Crosswalks provide a holistic analysis of laws and relevant standards. NIST uses crosswalks domestically to map laws and regulations, standards, and frameworks to help organizations facilitate and demonstrate conformance.[46] Other organizations (e.g., law firms and consultancies) have contributed to NIST's work in conducting crosswalks on California's Consumer Privacy Act, Virginia's Consumer Data Protection Act, the EU's GDPR, and Brazil's data protection law, as well as for the Fair Information Practice Principles and the International Association of Privacy Professionals' Certified Information Privacy Manager certification.[47] For example, NIST's crosswalk of the Privacy Framework and Cybersecurity Framework to its NIST Special Publication 800-53, Revision 5 identifies a catalog of security and privacy controls for information systems and organizations to protect operations and assets, individuals, other organizations, and the nation from a diverse set of threats and risks.[48] Similarly, NIST mapped its Cybersecurity Framework and the U.S. Health Insurance Portability and Accountability Act (HIPAA) to help firms identify gaps and potential tools.[49]

Standards crosswalks provide firms with a map to compare against their organization's legal and regulatory obligations and identify gaps and standards to demonstrate that an entity has taken concrete steps to meet regulatory obligations. Ideally, EU and U.S. officials, alongside private sector experts, could come together under a track 1.5 forum to discuss which international standards are most likely to be used by firms to show compliance under their respective legal and regulatory frameworks. This would help experts focus on the technical details rather than political objectives in trying to produce a deliverable for every TTC meeting. It would also hopefully prove sustainable over the long term (regardless of changes in administrations). The 1.5 track forum could develop a joint report to map out commonalities, differences, and gaps for further discussion and action.

Negotiate a Transatlantic Agreement on Law Enforcement Access to Data

The United States and EU could build on the enormous accomplishment that is the TDPF and conclude work on a new agreement—a U.S.-EU e-evidence/CLOUD Act agreement—to improve their respective law enforcement agencies' ability to access data held in each other's jurisdictions.[50] Thankfully, on March 2, 2023, the United States and EU announced the resumption of negotiations on an EU-U.S. agreement to facilitate access to electronic evidence in criminal investigations.[51] While the TDPF addresses transatlantic concerns about U.S. surveillance, a U.S.-EU e-evidence/CLOUD Act agreement would address concerns about U.S. law enforcement's (hypothetical) ability to access data under the U.S. CLOUD Act.

The United States and EU should provide similar high-level attention to newly restarted efforts on an e-evidence/CLOUD Act agreement as they did the forthcoming TDPF.

The TDPF undercuts France's rationale for its cloud sovereignty requirements (in terms of demanding immunity from U.S. national security law), as it uses the same "necessity and proportionality" standard utilized in Europe for conducting foreign intelligence surveillance.[52] Under the TDPF, the United States will create new administrative and judicial redress procedures for Europeans who consider their privacy rights to have been violated by U.S. surveillance agencies. These new measures establish essential equivalence between U.S. and EU law relating to foreign intelligence surveillance, and thereby directly address the concerns expressed by the Court of Justice of the European Union in Schrems II about the reach of U.S. authorities.

The United States negotiated CLOUD Act Agreements with the United Kingdom and Australia, both of which include additional legal safeguards for data privacy and other human rights.[53] The United States and EU said they'd work toward a new agreement in 2019, but progress stalled as Europe considered its intra-EU e-evidence act.[54] However, the EU just finalized the draft regulation and directive for the e-evidence act.[55] This provides a legal basis for EU member states to negotiate an agreement with the United States.

A U.S.-EU e-evidence/CLOUD Act agreement, though subject to new due process protections, would enable law enforcement to obtain e-evidence directly from providers of communications services (rather than relying on slow and antiquated government-to-government mutual legal assistance requests). Importantly, in the context of SecNumCloud and the EUCS proposal, an

agreement would hopefully mean Europe would not be able to claim law enforcement-related infringement of its sovereignty.

Allow the Mutual Recognition of U.S./EU Cybersecurity Certification and Auditing Programs

Just as the EUCS represents a legitimate effort to harmonize cloud cybersecurity certifications across the 27 EU member states, so too should the EU and United States work to build compatibility or mutual recognition into their respective cloud cybersecurity certification and auditing programs. Instead of enacting conflicting cybersecurity standards and processes, the two sides should use TTC to explore how they can align standards and accreditation and certification regimes. Ideally, this would entail mutual recognition of certifications. Yet, given how difficult this has proven to be in other areas, the two sides could at least work toward ensuring that firms accredited by one have a preferential path to accreditation in the other. Similarly, the United States and EU could work to recognize authorized third-party assessors from each side to make it somewhat easier for firms on either side to be audited for the other's cybersecurity certifications.

The Biden administration needs to start drawing lines in the sand and making it clear to EU officials that "enough is enough" when it comes to digital protectionism.

CONCLUSION

The French and EU sovereignty-based cloud cybersecurity regime poses a threat not just to transatlantic trade and technology cooperation but also to global technology governance, given how likely it is that other countries could adopt similar restrictions. If "trusted" cloud services means locally owned and controlled, then the potential for an open, innovative, and more secure global digital economy will be considerably diminished. European policymakers need to recognize what is at stake and the cost of misguided and counterproductive sovereignty restrictions not only to their own digital progress but also to continuing close transatlantic cooperation. Instead, they need to focus on the many areas where they can cooperate with their partners in the United States. For its part, the Biden administration needs to start drawing lines in the sand and making it clear to EU officials that "enough is enough" when it comes to digital protectionism.

Acknowledgments

The author wishes to thank Rob Atkinson, Stephen Ezell, and the cloud and cybersecurity experts who helped clarify the various cybersecurity programs. Any errors or omissions are the authors' responsibility alone.

About the Author

Nigel Cory (@NigelCory) is an associate director covering trade policy at ITIF. He focuses on cross-border data flows, data governance, and intellectual property and how they each relate to digital trade and the broader digital economy.

About ITIF

The Information Technology and Innovation Foundation (ITIF) is an independent, nonprofit, nonpartisan research and educational institute focusing on the intersection of technological innovation and public policy. Recognized by its peers in the think tank community as the global center of excellence for science and technology policy, ITIF's mission is to formulate and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress. For more information, visit us at itif.org.

ENDNOTES

1. Nigel Cory, "Testimony Before the U.S.-China Economic and Security Review Commission Regarding China's Cloud Computing Market" (Washington D.C., senate testimony, April 15, 2021), https://itif.org/publications/2021/04/15/testimony-us-china-economic-and-security-review-commission-regarding-chinas/.
2. Eline Chivot, "France's Airbnb Is Poised To Be Its Next Big Fail," Innovation Files, June 15, 2020, https://itif.org/publications/2020/06/15/frances-airbnb-poised-be-its-next-big-fail/; Victoria Shannon, "Quaero gets off the ground to challenge Google," *New York Times,* March 21, 2008, https://www.nytimes.com/2008/03/21/technology/21iht-quaero24.html; Emmanuel Paquette, "The French cloud in the middle of a storm," *L'Express,* June 15, 2016, https://lexpansion.lexpress.fr/high-tech/le-cloud-a-la-francaise-en-plein-orage_1802232.html.
3. Nigel Cory, "'Sovereignty Requirements' in French—and Potentially EU—Cybersecurity Regulations: The Latest Barrier to Data Flows, Digital Trade, and Digital Cooperation Among Likeminded Partners" (Cross Border Data Forum, December 10, 2021), https://www.crossborderdataforum.org/sovereignty-requirements-in-france-and-potentially-eu-cybersecurity-regulations-the-latest-barrier-to-data-flows-digital-trade-and-digital-cooperation-among-likemi/; Nigel Cory, "France's 'Sovereignty Requirements' for Cybersecurity Services Violate WTO Trade Law and Undermine Transatlantic Digital Trade and Cybersecurity Cooperation" (ITIF, May 10, 2022), https://itif.org/publications/2022/05/10/france-sovereignty-requirements-cybersecurity-services-violate-wto-trade/.
4. Nigel Cory, "Testimony Before the U.S.-China Economic and Security Review Commission Regarding China's Cloud Computing Market" (Washington D.C., senate testimony, April 15, 2021), https://itif.org/publications/2021/04/15/testimony-us-china-economic-and-security-review-commission-regarding-chinas/.
5. Netherlands National Cyber Security Centre, "'Small chance' of U.S. government accessing European data under CLOUD Act," November 23, 2022,

https://english.ncsc.nl/latest/weblog/weblog/2022/small-chance-of-u.s.-government-accessing-european-data-under-cloud-act.

6. Sylvain Roland, "'Cloud of trust': MP Philippe Latombe attacks the Google and Thales (S3ns) project with the CNIL and ANSSI," *La Tribune,* July 6, 2022, https://www.latribune.fr/technos-medias/internet/cloud-de-confiance-le-depute-philippe-latombe-attaque-le-projet-de-google-et-thales-s3ns-aupres-de-la-cnil-et-de-l-anssi-924750.html.
7. Michael Cabirol, "'On the trusted cloud, we are not talking about absolute sovereignty' (Guillaume Poupard, Anssi)," *La Tribune,* October 8, 2022, https://www.latribune.fr/entreprises-finance/industrie/aeronautique-defense/sur-le-cloud-de-confiance-on-ne-parle-pas-de-souverainete-absolue-guillaume-poupard-935510.html.
8. Both SecNumCloud and EUCS could impact government agencies and businesses across a broad range of sectors deemed "critical" and "vital."
9. For example, the U.S. Cybersecurity and Infrastructure Security Agency, the Department of Homeland Security, U.S. Computer Emergency Readiness Team (US-CERT), and others groups and initiatives depend on information sharing to help everyone do better in the face of ever changing cybersecurity threats. Likewise in Europe, information sharing is at the heart of the European Union's Agency for Cybersecurity, government agencies, EU-CERTs, and Information Sharing and Analysis Centers (ISACs) efforts to improve cybersecurity. ISACs are trusted entities to foster information sharing and good practices about physical and cyberthreats and mitigation. "US-CERT Info Sheet," CISA, https://www.cisa.gov/uscert/sites/default/files/publications/infosheet_US-CERT_v2.pdf; "U.S. Department of Homeland Security Cyber Information Sharing and Collaboration Program (CISCP)," CISA, https://www.cisa.gov/ciscp; "Information Sharing and Analysis Centers (ISACs)," ENISA, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing.
10. Going back to the 2004 launch of the International Watch and Warning Network, which was established to foster international collaboration on addressing cyberthreats, -attacks, and vulnerabilities. It provides a mechanism for participating countries to share information to build global cyber-situational awareness and incident response capabilities. In terms of data flow restrictions, see Nigel Cory and Luke Dascoli, "How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them" (ITIF, July 19, 2021), https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/.
11. Eugenia Lostri, James Lewis, and Georgia Wood, "A Shared Responsibility: Public-Private Cooperation for Cybersecurity" (CSIS, March 22, 2022), https://www.csis.org/analysis/shared-responsibility-public-private-cooperation-cybersecurity.
12. Cross-sector information sharing initiatives have often struggled historically. Many firms are reluctant to share information with the government, as doing so may include proprietary data and raise the risk of legal retaliation (whether from the government or due to financial oversight responsibilities). To address this, the U.S.'s 2015 Cybersecurity Information Sharing Act protects nonfederal organizations from liability for participating in sharing, as long as the process adheres to the law's standards.
13. Peter Swire and DeBrae Kennedy-Mayo, "The Effects of Data Localization on Cybersecurity" (June 24, 2022). *Georgia Tech Scheller College of Business*, Research Paper No. 4030905, https://ssrn.com/abstract=4030905 or http://dx.doi.org/10.2139/ssrn.4030905.
14. "ISO/IEC 27002:2022- Information security, cybersecurity and privacy protection — Information security controls," ISO, https://www.iso.org/standard/75652.html.
15. Emil Kiner and Satya Konduru, "How Google Cloud blocked the largest Layer 7 DDoS attack at 46 million rps," Google blog, August 18, 2022, https://cloud.google.com/blog/products/identity-security/how-google-cloud-blocked-largest-layer-7-ddos-attack-at-46-million-rps.

16. Julia Schuetze, "EU-US Cybersecurity Policy Coming Together: Recommendations for instruments to accomplish joint strategic goals" (EU Cyber Direct, November 25, 2020), https://eucyberdirect.eu/research/eu-us-cybersecurity-policy-coming-together-recommendations-for-instruments-to-accomplish-joint-strategic-goals: Catherine Stupp, "U.S., EU Plan Joint Foreign Aid for Cybersecurity to Counter China," *Wall Street Journal*, June 15, 2022, https://www.wsj.com/articles/u-s-eu-plan-joint-foreign-aid-for-cybersecurity-to-counter-china-11655285401.
17. FedRAMP brings the Federal Information Security Modernization Act of 2014 (FISMA) to life. "Federal Information Security Modernization Act of 2014," CISA, https://www.cisa.gov/federal-information-security-modernization-act.
18. Michael McLaughlin, "Reforming FedRAMP: A Guide to Improving the Federal Procurement and Risk Management of Cloud Services" (ITIF, June 15, 2020), https://itif.org/publications/2020/06/15/reforming-fedramp-guide-improving-federal-procurement-and-risk-management/.
19. "Understanding Baselines and Impact Levels in FedRAMP," FedRAMP, November 16, 2017, https://www.fedramp.gov/understanding-baselines-and-impact-levels/.
20. NIST's Federal Information Processing Standard 199, which defines three ways of securing data according to confidentiality, availability, and integrity. Department of Commerce, "Standards for Security Categorization of Federal Information and Information Systems," February 2004, https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf.
21. Ibid.
22. Ibid.
23. By JAB. "Pursuing a FedRAMP JAB Provisional Authorization," FedRAMP, https://www.fedramp.gov/jab-authorization/.
24. Again, this is based on a NIST standard, namely, NIST Special Publication 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems and Office of Management and Budget circular A-130, Managing Information as a Strategic Resource.
25. "FedRAMP Continuous Monitoring Strategy Guide Version 3.2," FedRAMP, April 4, 2018, https://www.fedramp.gov/assets/resources/documents/CSP_Continuous_Monitoring_Strategy_Guide.pdf.
26. JAB members include the chief information officers from the Department of Defense, Department of Homeland Security, and General Services Administration.
27. "FedRAMP Marketplace," FedRAMP, https://marketplace.fedramp.gov/#!/assessors?sort=assessorName.
28. "ISO/IEC 17020:2012 — Conformity assessment — Requirements for the operation of various types of bodies performing inspection," ISO, https://www.iso.org/standard/52994.html.
29. These provide a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the United States from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. U.S. National Institute of Standards and Technology, "SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations," September, 2020, https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.
30. "FedRAMP's NIST Rev5 Transition Plan," FedRAMP, November 24, 2020, https://www.fedramp.gov/FedRAMP-NIST-Rev5-Transition-Plan/.
31. Under control SA-9(5)). SA-9 (5)-1 [information processing, information data, AND information services], SA-9 (5)-2 [U.S./U.S. Territories or geographic locations where there is U.S. jurisdiction], SA-9 (5)-3 [all High impact data, systems, or services]. The organization restricts the location of

[FedRAMP Selection: information processing, information data, AND information services] to [FedRAMP Assignment: U.S./U.S. Territories or geographic locations where there is U.S. jurisdiction] based on [FedRAMP Assignment: all High Impact Data, Systems, or Services].

32. German Federal Office for Information Security, "Cloud Computing Compliance Controls Catalogue (C5)," https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CloudComputing/ComplianceControlsCatalogue-Cloud_Computing-C5.pdf.
33. Daniel Castro, "The False Promise of Data Nationalism" (ITIF, December 9, 2013), https://itif.org/publications/2013/12/09/false-promise-data-nationalism/.
34. The hack on the US. Office of Management and Budget (OMB) occurred, at least in part, in an on-premises environment as a result of compromised user credentials. While the AWS report does not specify that it was referring to the OMB hack, it is more than likely the example it refers to. It's fairly clear from the agency OIG reports that OMB was running a number of its own data centers and that it was behind on security. Min Hyun, "Addressing Data Residency with AWS," AWS Blog post, February, 2018, https://aws.amazon.com/blogs/security/addressing-data-residency-with-aws/; The Majority Staff Report, "The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation" (Committee on Oversight and Government Reform U.S. House of Representatives 114th Congress, September 7, 2016), https://republicans-oversight.house.gov/report/opm-data-breach-government-jeopardized-national-security-generation/.
35. Canada is unique in its clear and explicit articulation of "data sovereignty" in relation to government data and services. It requires cloud services to keep certain categories of sensitive and classified data within Canada. It does not necessarily apply to data in transit, as Canada recognizes that certain cloud services may only be run outside Canada. These requirements are included in Canada's public service cloud contracts. AWS and other U.S. cloud firms with data centers in Canada have won contracts given they have local data centers. "Government of Canada White Paper: Data Sovereignty and Public Cloud," Canada.ca, https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/gc-white-paper-data-sovereignty-public-cloud.html; Reginald Maltais, "Protected workloads on public cloud," Statistics Canada, July 25, 2022, https://www.statcan.gc.ca/en/data-science/network/cloud-workload.
36. The U.S. government has issued, and plans further, several executive orders that address how to improve cybersecurity in critical infrastructure sectors. "Executive Order on Improving the Nation's Cybersecurity," whitehouse.gov, May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.
37. Theodore Christakis (Twitter): "A real battle is going on re @enisa_eu draft cybersecurity certification scheme for #cloud services & FR push to include sovereignty, data localization & 'immunity from non-EU Laws' requirements. @POLITICOEurope reports IE SE NL express 'serious concerns' cc #CloudAct #SchremsII," Twitter, April 8, 2022, https://twitter.com/TC_IntLaw/status/1512339491092062216.
38. Andrew Harvey, Fiona Willis, and Stefano Mazzocchi, "European Cybersecurity Certification Scheme for Cloud Services (EUCS) – Solutions on the Issue of Independence to Non-EU Law," The Association for Financial Markets in Europe, March 13, 2023, https://www.afme.eu/Portals/0/DispatchFeaturedImages/230310_AFME Comments on EUCS_FINAL.pdf.
39. "NIST Asks Public to Help Future-Proof Electronic Information," NIST, December 20, 2016, https://www.nist.gov/news-events/news/2016/12/nist-asks-public-help-future-proof-electronic-information; "PQC Standardization Process: Announcing Four Candidates to be Standardized, Plus Fourth Round Candidates," NIST, July 5, 2022, https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4.
40. Multi-trade association letter, "European Cybersecurity Certification Scheme for Cloud Services," ITIC, June 14, 2022, https://www.itic.org/documents/europe/Final_EUCS_statement_1406.pdf;

Laura Kabelka, "Sovereignty requirements remain in cloud certification scheme despite backlash," *Euractiv*, June 16, 2022, https://www.euractiv.com/section/cybersecurity/news/sovereignty-requirements-remain-in-cloud-certification-scheme-despite-backlash/; Plus the various letters from Germany, Ireland, Sweden, and the Netherlands about EUCS and ENISA's development of it.

41. Laura Kabelka, "Sovereignty requirements remain in cloud certification scheme despite backlash," *Euractiv,* June 16, 2022, https://www.euractiv.com/section/cybersecurity/news/sovereignty-requirements-remain-in-cloud-certification-scheme-despite-backlash/.
42. Contained in EUCS Annex J.
43. Luca Bertuzzi (@BertuzLuca on Twitter), "#EUCS: EU cyber attaches visited ENISA's HQ last week. The agency anticipated that a potential compromise on the cloud cybersecurity scheme could consist in splitting the level of assurance high into two subgroups," November 16, 2022, https://twitter.com/BertuzLuca/status/1592874026183319552.
44. Laurens Cerulus, "Big Tech cries foul over EU cloud-security label." *Politico,* June 14, 2022, https://www.politico.eu/article/tech-sector-foul-eu-cloud-security-label/.
45. Nigel Cory, "'Sovereignty Requirements' in French—and Potentially EU—Cybersecurity Regulations: The Latest Barrier to Data Flows, Digital Trade, and Digital Cooperation Among Likeminded Partners" (Cross Border Data Forum, December 10, 2021), https://www.crossborderdataforum.org/sovereignty-requirements-in-france-and-potentially-eu-cybersecurity-regulations-the-latest-barrier-to-data-flows-digital-trade-and-digital-cooperation-among-likemi/; Nigel Cory, "France's 'Sovereignty Requirements' for Cybersecurity Services Violate WTO Trade Law and Undermine Transatlantic Digital Trade and Cybersecurity Cooperation" (ITIF, May 10, 2022), https://itif.org/publications/2022/05/10/france-sovereignty-requirements-cybersecurity-services-violate-wto-trade/.
46. "Crosswalks," NIST, https://www.nist.gov/privacy-framework/resource-repository/browse/crosswalks.
47. Ibid.
48. "NIST Privacy Framework and Cybersecurity Framework to NIST Special Publication 800-53, Revision 5 Crosswalk," NIST, https://www.nist.gov/privacy-framework/nist-privacy-framework-and-cybersecurity-framework-nist-special-publication-800-53.
49. "HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework," United States Department of Health and Human Services, February 22, 2016, https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf.
50. Kenneth Propp, "Has the Time for an EU-U.S. Agreement on E-Evidence Come and Gone?" Lawfare blog, June 2, 2022, https://www.lawfareblog.com/has-time-eu-us-agreement-e-evidence-come-and-gone.
51. "EU-U.S. announcement on the resumption of negotiations on an EU-U.S. agreement to facilitate access to electronic evidence in criminal investigations," European Commission, press release, March 2, 2023, https://commission.europa.eu/news/eu-us-announcement-resumption-negotiations-eu-us-agreement-facilitate-access-electronic-evidence-2023-03-02_en.
52. Kenneth Propp, "European Cybersecurity Regulation Takes a Sovereign Turn," European Law Blog, September 12, 2022, https://europeanlawblog.eu/2022/09/12/european-cybersecurity-regulation-takes-a-sovereign-turn/.
53. Jennifer Daskal and Peter Swire, "The U.K.-U.S. CLOUD Act Agreement Is Finally Here, Containing New Safeguards," Lawfare blog, October 8, 2019, https://www.lawfareblog.com/uk-us-cloud-act-agreement-finally-here-containing-new-safeguards.
54. Luca Bertuzzi, "EU co-legislators agree on 'key elements' of electronic evidence package," *Euractiv,* June 29, 2022, https://www.euractiv.com/section/digital/news/eu-co-legislators-agree-on-key-elements-of-electronic-evidence-package/; Kenneth Propp, "Has the Time for an EU-U.S. Agreement

on E-Evidence Come and Gone?," Lawfare blog, June 2, 2022, https://www.lawfareblog.com/has-time-eu-us-agreement-e-evidence-come-and-gone.

55. Council of the EU, "Electronic evidence: Council confirms agreement with the European Parliament on new rules to improve cross-border access to e-evidence," press release, January 25, 2023, https://www.consilium.europa.eu/en/press/press-releases/2023/01/25/electronic-evidence-council-confirms-agreement-with-the-european-parliament-on-new-rules-to-improve-cross-border-access-to-e-evidence/.