EXPLAINER

European Cybersecurity Certification Scheme for Cloud Services (EUCS)

Cybersecurity Legislative Analysis Series

Bill Summary: Establishes cybersecurity requirements for secure and interoperable cloud services within the European Union (EU)

Latest draft updated March 22, 2024, with possible adoption by European Cybersecurity Certification Group on April 15, 2024

Rating: CYBER NEUTRAL This bill has potential to improve the safety and security of cloud service providers but risks limiting non-EU-based companies from operating successfully in Europe.

Last updated: April 4, 2024

Key Provisions

- Aims to enhance and streamline cloud services cybersecurity guarantees across four levels of assurance (basic, substantial, high, high+) and across all kinds of cloud services (Infrastructure as a Service, Platform as a Service, and Software as a Service, among others) across the EU
- Serves as a technical tool designed to assist customers make informed decisions through the establishment of cybersecurity best practices for cloud service providers (CSPs) to protect data and services hosted in the cloud
- Requires CSPs to undergo a certification process resulting in a three-year renewable certification; adherence requires periodic audits
- Provides EU customers with a holistic view of risk of prospective CSPs; CSPs seeking the highest certification level will file an "International Company Profile Attestation" (ICPA) to indicate which jurisdiction(s) they are subject to, which will then be communicated to customers
- Allows EU member states to include sovereignty requirements in the attestation, which could be incorporated into contractual agreements without impacting certification

Background

The EU's Cybersecurity Act established a voluntary cybersecurity certification framework for products and services. The law tasked the EU Agency for Cybersecurity (ENISA) with developing EU-wide voluntary cybersecurity certification schemes to regulate CSPs (among others, such as 5G technology and artificial intelligence) and to harmonize the security and interoperability of cloud services with EU regulations, international standards, and industry best practices. Of the three certificate schemes proposed, only one (on baseline information and communication technology products) has been approved to date.

The certification scheme is broken down into four levels of assurance—basic, substantial, high, and high+—each determined by the level of risk associated with the intended use of the cloud service plus five other factors: suitability, attacker profile, scope, depth, and rigor. Basic level is a minimum acceptable baseline for cloud cybersecurity; substantial level includes more enhanced security measures; high level is designed for cloud services that handle highly sensitive data or critical operations; and high+ level requires the most stringent security controls and requirements.

Initial drafts of the EUCS included sovereignty requirements compelling CSPs to localize their cloud services by headquartering in the EU, to store European data within the EU, and to only allow organizations with "high+" certification to access that data. This development stemmed from a concern over potential U.S. surveillance and law enforcement access to cloud data, and it would have excluded

EXPLAINER

European Cybersecurity Certification Scheme for Cloud Services (EUCS)

Cybersecurity Legislative Analysis Series

Background (continued)

non-EU CSPs from providing services to EU cloud customers. With immense pushback from some EU member states, overseas and European industry groups, lobbyists, technology companies, and analysts, subsequent updated drafts amended this requirement so that only CSPs seeking a "high+" assurance level are required localize their data, with the possibility of allowing "trusted foreign cloud providers" to be certified.

Though stakeholders were still dissatisfied, ongoing negotiations finally led to the removal of sovereignty requirements (replaced by attestation for CSPs seeking a "high" level of certification) in the latest draft, dated March 22, 2024. The attestation will be verified and validated by the Conformity Assessment Body (CAB). Sovereignty requirements may still be applied by individual EU member states but will not impact the certification process. The next expert group meeting is scheduled for April 15, when the European Cybersecurity Certification Group will likely agree to the text and proceed toward implementation.

Key Takeaways

- The certification scheme is given a neutral rating due to the highly politicized nature of the debate over sovereignty. This three-year deadlock detracted from answering questions about the cybersecurity requirements themselves, scheme implementation, and standards harmonization across the EU, all of which may have attendant effects on the region's cybersecurity and resilience.
- While technically voluntary, Europe's Network and Information Security (NIS2) Directive requires that cloud customers only utilize cloud services certified by the EUCS. Potential private-sector customers may also require EUCS certification as a procurement requirement, thereby making the certification mandatory to conduct business.
- CSP attestation of applicable jurisdictions could promote transparency and allow cloud services customers the potential to conduct a more holistic risk assessment, but it highlights a trust disparity between EU member states and the United States regarding potential extraterritorial access to data. Other agreements like the Budapest Convention's Second Additional Protocol, the Organization for Economic Cooperation and Development's Declaration on Government Access to Personal Data Held by Private Sector Entities, and the United States' Clarifying Lawful Overseas Use of Data (CLOUD) Act will hopefully provide further clarity in this realm.

Cybersecurity Analysis

FACTORS	ANALYSIS
Applicability	The certification system would apply to any CSP seeking to provide products or services to EU customers.
Impact on cyber actions	The distinction between functional requirements and sovereignty statements will be crucial for the effective implementation of the scheme. The EUCS and supporting regulatory bodies should assist customers in making risk-informed judgments for the procurement of cloud services and products. Security objectives and requirements are stipulated in EUCS Annex A: Security Objectives and Requirements for Cloud Services. Any CSP that does not meet baseline cybersecurity standards will likely face issues obtaining certification from the CAB.

European Cybersecurity Certification Scheme for Cloud Services (EUCS)

Cybersecurity Legislative Analysis Series

Cybersecurity Analysis (continued)

FACTORS	ANALYSIS
Business impact	While technically voluntary, the certification scheme will likely be mandatory for successfully conducting business in the EU, or any CSPs that would serve sensitive sectors such as energy or finance (i.e., highly critical sectors designated in the NIS2). After the EUCS is implemented, there will be some business cost associated with understanding the full scope of the scheme and compliance to its requirements. At this time, it is unclear how the ICPA process will ultimately impact EU customers of cloud services and products or how it will affect the ability of CSPs with outside jurisdictional obligations to conduct business within the EU.
Data privacy and data security	In its filing of an ICPA, CSPs would be required to provide information about the location of the storage and processing of their customers' data and to indicate which jurisdiction(s)' laws they are subject to. While this procedural step does not inherently change data security or data privacy standards, it may apply pressure for CSPs to adhere to best practices in data security and privacy.
Rulemaking or update mechanisms	The European Commission originally requested that ENISA add sovereignty requirements to the EUCS, such as that CSPs would have their "registered head office and global headquarters … in a Member State" and be required to demonstrate legal immunity from foreign jurisdictions—an impossibility for any U.S.-based company to comply with while also remaining consistent with U.S. law. This requirement has since been removed. For those seeking a "high" level of certification, CSPs must file an ICPA to determine which sovereignty regime they would be subject to. Member states can include their national legislation on sovereignty and incorporate their national requirements into contractual agreements. Regulatory authorities within each EU country will likely be responsible for EUCS enforcement. The draft text states "Enforcers will in particular need to verify that cloud service providers comply with the parts of the regulation that depend on the scheme." However, the decision on whether ENISA, the European Commission, or the EU Parliament and Council will be in charge of determining cloud certification requirements remains unresolved. Some opponents of EUCS argue that the scheme should be discussed as a political matter rather than a regulatory issue that ENISA alone would decide.
Enforcement mechanisms	EUCS can be enforcement-heavy, requiring CSPs to certify and be subject to periodic audits throughout the certification term. The process also involves the CAB, which evaluates CSPs' ICPA statements and determines their certification level. Prospective business agreements are also subject to each EU member state's national sovereignty requirements, should they have any.
Other notes	At this time, it is unclear whether the "high+" category will remain after the negotiated March 2024 draft introduced updated ICPA and CAB processes.