Our position

Cybersecurity Certification Scheme for Cloud Services (EUCS)

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate US investment in Europe totalled more than €3.7 trillion in 2022, directly supports more than 4.9 million jobs in Europe, and generates billions of euros annually in income, trade and research and development.

American Chamber of Commerce to the European Union
Speaking for American business in Europe

Avenue des Arts/Kunstlaan 56, 1000 Brussels, Belgium • **T** +32 2 513 68 92
info@amchameu.eu • amchameu.eu • European Transparency Register: 5265780509-97

Executive summary

Sovereignty requirements continue to form an integral part of the latest draft of the Cybersecurity Certification Scheme for Cloud Services (EUCS). These discriminatory global headquarters and ownership requirements provoked significant concern amongst industry as well as among the EU's security and trade partners. Before the European Cybersecurity Certification Group (ECCG) can consider approving the EUCS as a candidate scheme for the European Commission, the European Union Agency for Cybersecurity (ENISA) should clarify certain concerns about the proposal. Given the public disagreement about the sovereignty controls and the extensive impact they will have on the cloud market[1] and, by extension, on many of the entities in scope of the NIS2, the EUCS requires an impact assessment. In particular, it should be explained how the different levels of assurance will impact workloads and critical entities using cloud services, as well as the reasoning behind applying different levels of assurance. To further inform and assist policymaker's work, this document also contains a series of suggested amendments.

Industry concerns[2]	**Limited transparency and lack of stakeholder engagement**	**Inclusion of 'digital sovereignty' requirements**	**Conflicting Member States' views**	**Legal confusion and uncertainty caused by the interplay with other EU legislation**	**Compliance with a World Trade Organisation (WTO) rules**

Introduction

The latest draft of the EUCS still contains the sovereignty requirements, previously known as Independence from Non-EU Laws. They are currently incorporated in Annex J titled 'Protection of European Data against Unlawful Access' (PUA), and cause discriminatory global headquarters and ownership requirements. The addition of the new Evaluation Level 4 (EL4) in the new draft creates a further layer of complexity and does to not conform with article 52 of the EU Cybersecurity Act (CSA), which provides for three assurance levels.

[1] Continued inclusion of a prohibition on non-EU Headquartered cloud operators presents serious risk of capacity shortfall and trade retaliation. The WTO Agreement on Government Procurement prohibits Member States from blocking foreign-owned firms from participating in public sector markets ex ante, and the EU's commitments under the WTO General Agreement on Trade in Services ("GATS") include obligations on national treatment and most-favored nation that would also likely prohibit such policies. Moreover, a recent ECIPE study estimates that a full ban on cross-border data flows of only personal data from the EU to the US could result in a 31% decline in digital services imports from the US to the EU – a substantial impact given that digital services account for 39% of the total US exports to the EU. It is highlighted that substitution of imports of some of the world's most advanced and most internationally competitive digital services from the US would be unlikely in the short- and medium-term, especially where there is a lack of established and globally competitive providers outside the US. Overall, it is estimated that company productivity will decline in the EU. On aggregate, the impact of a ban on cross-border data flows outside the EU could have a huge long-term impact, ranging from an estimated 1.9% to 3.0% of EU GDP. See study by ECIPE here: https://ecipe.org/publications/resilience-cybersecurity-economic-trade-impacts-cloud-immunity/ .

[2] See our latest join-industry statement on the need for a swift adoption of the EU Cybersecurity Certification Scheme for Cloud Services without sovereignty requirements here: http://www.amchameu.eu/position-papers/joint-industry-statement-need-swift-adoption-eu-cybersecurity-certification-scheme

Furthermore, the new draft does not resolve the numerous questions that have been raised by Member States, trade associations, academics, and industry stakeholders, including AmCham EU[3]. These include the practical effects and internal market impacts of the sovereignty controls on European economic and security interests, the intended scope of these controls, conformity with the requirements of the CSA and the scope and applicability of these requirements. Moreover, even Evaluation level 3 (EL3) is subject to the Annex J EL4 requirements. In sight of these concerns, at AmCham EU we would like to provide key suggestions for improvement.

Scope of new Evaluation Level 4 (EL4)

The proposed scope for the newly suggested EL4 applies to 'data of particular sensitivity'. Page 32 of the draft scheme covers a very broad range of workloads and interferes with EU Member States' exclusive competences (eg proceedings before courts, protection of privacy, medical secrecy and public health data, intellectual property, economic and financial information et. al.).

This scope lacks a sufficiently narrow and precise definition of which workloads would be subject to the associated EL4, as it the case for the other levels. This has been called out by the wider industry. The proposed definitions suggest a very broad scope of application. In addition to data related to national security and classified government information, ENISA also includes the following categories in scope for EL4: 'the protection of privacy, to medical secrecy, and to trade secrets, which includes the secrecy of production methods, economic and financial information, and of information on commercial or industrial strategies'. These are areas where European Union does not have competence under the CSA, since it concerns national security and defence or merely has supportive competence with no authority to adopt a binding legal act. EL4 therefore suggests requirements that go far beyond the scope of the European CSA and further lack the proper assessment on proportionality and subsidiarity, as required by the EU treaties (art. 5 [3] TEU).

Additionally, EL4 remains too vague to properly assess. For example, EL4 also refers to 'health, or the protection of intellectual property'. This list of use cases is open to very broad interpretation that expands far beyond national security and classified information into a wide range of economic and public service contexts, which could result in diverging applications by EU Member States. This is exactly the opposite to what the EUCS aims to achieve as a pan- European scheme.

Before the ECCG can consider to approve the EUCS as a candidate scheme to be handed over formally to the European Commission, we outline a number of challenges and questions that ENISA should clarify:

Questions to ENISA:

1. How does ENISA reconcile its stated desire for a very narrow scope with the inclusion of seemingly broad, catch-all data categories cited in the draft?
2. How does ENISA envisage that a final definition on scope will be reached? If this is left to Member States or sectoral legislation to define, this will likely fail to deliver the harmonised

[3] See our latest join-industry statement on the need for a swift adoption of the EU Cybersecurity Certification Scheme for Cloud Services without sovereignty requirements here: http://www.amchameu.eu/position-papers/joint-industry-statement-need-swift-adoption-eu-cybersecurity-certification-scheme

framework that the EUCS sets out to achieve. As currently drafted, the definition seems to cross Member State competences (national security) and EU competences, making it unclear where authority resides to set the scope.

3. Article 1 of the CSA provides ENISA with the following mandate: 'This Regulation is without prejudice to the competences of the Member States regarding activities concerning public security, defence, national security and the activities of the State in areas of criminal law'. EL4 is referring to topics that go beyond the scope of the EU Cybersecurity Act. How does ENISA explain that EL4 sets requirements for data related to national security and classified government information, and the protection of privacy, to medical secrecy, and to trade secrets, which includes the secrecy of production methods, economic and financial information, and of information on commercial or industrial strategies. Has ENISA performed a legal analysis if the EUCS complies with the primary objective and scope of the CSA and that EUCS, as a technical instrument, can to set legal requirements which go beyond article 1?

The framing of EL4 and conformity with the Cybersecurity Act

Whilst the CSA provides the ability to develop evaluation levels alongside the very clear requirement for a three-tiered assurance framework, it is unclear that what ENISA proposes that for EL4 constitutes an 'evaluation level' and not a *de facto* fourth 'assurance level'. Assurance levels differ in correspondence to the risk and significance of impact associated with an incident for a particular Information Communication Technologies (ICT) use case (art.52[1] CSA). Evaluation levels differ based on the level of 'rigour and depth' of analysis that is required for particular uses (Recital 66, CSA). The natural inference of ENISA's scoping of EL4 to 'the most sensitive uses of cloud services' is that this level of the market features unique security risks wherein the impact of an incident would threaten national security, public order, health etc. This would appear to correspond to a distinct risk profile in keeping with the spirit of an assurance level. It is not clear that what differentiates Annex J controls is the rigour and depth of evaluation applied at different levels. In the case of the non-EU operator Control Requirements the difference is not in the rigorousness of evaluation applied at assurance level higher than other levels - it is in the fact that this criteria only applies to level high and not to any degree of rigor at other levels. Moreover, we recommend to revise evaluation level 3 (EL3) to only focus on risk-based security requirements while avoiding any overlap with EL4. Further clarification is needed on the following issues:

Questions to ENISA:

1. Did ENISA perform a legal analysis prior to suggesting adding a fourth layer of assurance, referred to as EL4?

2. ENISA appears to frame evaluation level 4 in relation to a unique risk profile. On what grounds does it consider this an evaluation level rather than an assurance level?

Comments and proposed amendments

Page	Issue	Comments and proposed amendments
13	'The EUCS aims at making core geographical and legal information about the cloud services available and understandable to all users of the scheme to allow to use them as needed;'	• Being transparent about where data is processed is a clear ask. However, the proposed requirements in ANNEX H/J go above and beyond, asking the Cloud Service Provider (CSPs) for example also to consider only LEA requests from EU Member States or based on EU law only – and this even for a EL3.
14	EUCS is too complex and demanding to stimulate cloud uptake in Europe 'Additional information from the Commission request to develop the scheme. In the request to prepare the scheme, the Commission asks ENISA to "(…) prepare a candidate European cybersecurity certification scheme for cloud services." In addition, the request is justified by the need to "stimulate cloud uptake in Europe" as "cloud computing is an underlying technology for any development in technological fields.'	• How is the scheme which talks about 4 different levels of security going to stimulate cloud uptake in Europe? Won't that added complication make cloud adoptability more difficult? Will also the broad scope for EL4 not lead to a fragmentation of the Single Market, due to cherry picking of what data Member State may apply for EL4? • This current version of the EUCS requires severe investment in compliance resources from all CSPs, big and small. Additionally, it provides no guidance to customers of CSPs about which assurance level they should seek in order to leverage the cloud. It could cause confusion and provide advantages to those who can conform to CS-EL3. Customers deserve the best possible state of the art security and resilience. Security is a business enabler – data localization has no value added on how secure or resilient your data

		is. data, you don't have a business in providing cloud services.
14	'In the evaluation of a cloud service, the EUCS shall support and encourage the reuse of conclusions and objective evidence from already audited or certified ICT products, ICT processes, and ICT services, in particular those cloud services that have been certified with the EUCS:'	- Despite this text in the scheme ~~the above~~, ENISA has suggested to disassociate the EUCS requirements from existing security certifications such as 27001.
15	'The EUCS is intended to be a horizontal scheme, applying requirements based on the same security objectives to all cloud services, covering the EUCSA's three assurance levels;'	- The suggested new 4th / or sub level in high assurance is inconsistent with this statement referring to the 3 legally defined levels in the Cybersecurity Act. Furthermore, as shared by ENISA, the intention of the EUCS is NOT to apply to ALL cloud services.
15	'The EUCS is a technical tool designed to provide information to customers and allow them to make informed decisions. As such, the EUCS only enforces restrictions on geographical location of data or processing, or on applicable laws at evaluation level CS-EL4; however, it requires the CSP to be transparent about this information at all evaluation levels, and to make it publicly available and understandable as part of the information provided with the certificate.'	- Seems incompatible with the idea that our existing customers would expect the highest security applied to the cloud services that we provide to them and yet we cannot certify against the highest assurance levels of EUCS.
16	'Another important aspect of certification is related to the split of responsibility between the CSP and the CSC (Customer). The fulfilment of the requirements by the CSP's cloud services is evaluated under the assumption that the CSC follows the	- Is it realistic to assume that a Cloud Services Customer will follow all the security recommendations provided by CSP? Don't they need to be made aware about the importance of these recommendations? And who is responsible for this? And

	recommendations provided by the CSP in the cloud service's documentation.'	who will be responsible for the cybersecurity incidents which occur because of the lack of awareness/resources on the CSC's part?
17	'The EUCS aims at improving the EU Internal Market conditions, and at enhancing the level of cybersecurity of a wide range of cloud services, of the cloud capabilities types they implement, including application, infrastructure, and platform capabilities. The EUCS covers a wide range of cybersecurity requirements, by offering evaluation levels corresponding to all three (3) assurance levels defined in the EUCSA ("basic", "substantial" and "high").'	• Cybersecurity of cloud services is a secondary objective.
23	'The standards that are referenced are very classical in the IT security field, but in most cases, it has not been possible to apply the standards directly, and new specifications have been defined.'	• Most CSPs are able to apply existing standards and would be able to achieve a high Assurance Level were it to be defined properly. The distinction between say substantial and high is not grounded in a measurable improvement in security. ~~and~~ a • A risk based approach to security would not result in 3 discrete levels of security and is more effective at addressing an evolving threat landscape.
32	'The CS-EL4 level provides reasonable assurance that a set of security controls is designed and operated in a way that goes beyond the CS-EL3 level to address security risks and threats related to data of particular sensitivity that would present risks to society if breached. The data of particular sensitivity mentioned above cover: - data related to secrets protected by law, for example, secrets relating to	**Suggested amendment:** 'The CS-EL4 level could provide ~~reasonable~~ assurance that a set of security controls is designed and operated in a way that goes beyond the CS-EL3 level to address security risks and threats related to data of particular sensitivity that would present ~~risks to society if breached.~~ risks to national security. The data of particular sensitivity mentioned above cover:

	the deliberations of the Government and of the authorities reporting to the executive branch, to national defense, to foreign policy, to national security, to proceedings before the courts, or to the protection of privacy, to medical secrecy, and to trade secrets, which includes the secrecy of production methods, economic and financial information, and of information on commercial or industrial strategies; - data that are necessary for the accomplishment of essential State functions, in particular the safeguarding of national security, the maintenance of public order and the protection of human life and health.’	- data related to secrets protected by law, for example, secrets relating to the deliberations of the Government and of the authorities reporting to the executive branch, to national defence, to foreign policy, to national security, to proceedings before the courts~~, or to the protection of privacy, to medical secrecy, and to trade secrets, which includes the secrecy of production methods, economic and financial information, and of information on commercial or industrial strategies;~~ - data that are necessary for the accomplishment of essential State functions, in particular the safeguarding of national security, the maintenance of public order and the protection of human life and health.’ **Justification:** • The above definition of ‘data of particular sensitivity’ is too broad and unclear as it includes multiple EL4 categories, which would be typical for the highest critical infrastructures. Given that J.2.4 PUA-04 Control requirements under Annex J apply to EL4, the definition and scope of ‘data of particular sensitivity’ should be limited to data which, if compromised, may have an impact on defence, national security, state secrets, classified information. Otherwise, the broad applicability of J.2.4 PUA-04 Control requirements would be too broad and risk creating significant barriers of entry to non-EU headquartered cloud service providers in a disproportionate manner. Many European sectors are dependent on state-of-the-art cloud technologies for their own operational resilience and competitiveness. By potentially

		limiting the choices of cloud security technologies available for European governments and companies in the Single Market, the purpose of the EUCS to enhancing the level of cybersecurity of a wide range of cloud services, and therefore improving European resilience to cyberattacks overall, is jeopardised.
206	The CSP shall provide comprehensible and transparent information on: • Its jurisdiction; and • System component locations, including its subservice providers, where CSC data, meta-data, cloud service derived data and CSC account data is processed, stored and backed up; • **System component locations, including for its subservice providers, where any CSP data is processed, stored, and backed up;** • The locations from which administration and supervision may be carried out on the cloud service. • **The locations from which the CSP conducts support operations for CSCs, including the list of operations that can be carried by support teams in each location.** The CSP shall provide sufficient information for subject matter experts of the CSC to determine and to assess the suitability of the cloud service's jurisdiction and locations from a legal and regulatory perspective.	**Suggested amendment:** The CSP shall provide comprehensible and transparent information on: • Its jurisdiction; and • System component locations, including its subservice providers, where CSC data, ~~meta-data, cloud service derived data and CSC account data~~ is processed, stored and backed up; • **System component locations, including for its subservice providers, where any CSP data is processed, stored, and backed up;** • The locations from which administration and supervision may be carried out on the cloud service. • **The locations from which the CSP conducts support operations for CSCs, including the list of operations that can be carried by support teams in each location.** The CSP shall provide sufficient information for subject matter experts of the CSC to determine and to assess the suitability of the cloud service's jurisdiction and locations from a legal and regulatory perspective.

		Justification Obliging a CSP to offer at least one option where the storing and processing of meta-data and cloud derived data does not give security or privacy benefits. This obligation appears to be disproportionate to the objective Annex J aims to achieve, which is about protecting European data from unlawful access. It is already a best practice in the EU market to process and store CSC data, for example in a dedicated cloud Multi-Zone-Region. However, it should be the client's choice whether to extend such localisation requirements also to meta-data and cloud service derived data, which is distinct data from CSC data.
301	'The CSP shall state in contractual documents with CSCs that the CSP shall only consider investigation requests related to the provision of the cloud service that are issued upon EU law or EU Member State law.'	'The CSP shall state in contractual documents with CSCs that the CSP shall only consider legally valid investigation requests for CSC data. CSPs shall implement measures to address such requests, including, notifying CSC, where permissible, of legally valid requests for CSC data to enable the CSC to take necessary actions to communicate directly with the relevant authority to respond to such request.' **Justification** - The original wording appears to be disproportionate and virtually impossible from a legal perspective to adhere to for any CSP that has operations in jurisdictions outside of the EU. This also includes European CSPs with business operations in non-EU jurisdictions and could possibly not even allow EU headquartered CSPs to qualify against EL3. The new wording is aligned with best-practice legal safeguards that CSPs already implement to protect their clients' data in Europe and as part of their

		commitments to mitigate risks associated with government requests for data.
ANNEX A	'The content of sections A.2 to A.22 of the present annex has been submitted to CEN-CENELEC JTCS13's WG2 for adoption as a Technical Specification. The discussions are under way, and if a Technical Specification is adopted that matches the expectations of the EUCS, the requirements in this Annex will be replaced by a reference to the adopted Technical Specification.'	• The Annex A material is not the latest from JTC13 and as per the work in JTC13 only considers 3 assurance levels – basic, substantial, high. There is a clear governance question: Where lies responsibility for deciding that the TS meets the expectations of EUCS? Is that ENISA? One of the sensitivities of the work in JTC13 is the constant reminder from ENISA that if this TS doesn't work for them, they don't have to use it. This has meant us CSPs have had to tread a bit carefully during JTC13 discussions The TS is not aligned with how standards are developed in CEN/CENELEC and in particular the referencing of existing standards due to the insistence of ENISA to disassociate EUCS from existing standards. • The EUCS certification scheme Annex A should only reference the TS from CEN/CENELEC and NOT replicate the text of the TS. This enables ongoing maintenance of the TS to ensure that it is aligned with updated security practices.
ANNEX J	Control requirements shifted without clear motivation or impact assessment.	• The previous eligibility requirements from SNC which were in J.2.1 and applied to level high are now in J.2.4 and applied to CS-EL4 and now referred to as 'control requirements'.
	Primacy of EU Law now added in the lowest level of assurance, without clear motivation or impact assessment.	Contracts between CSP/CSC under EU law to be applied from the Basic level (previously from level high only).

Conclusion

Since 2021, industry has called the European Commission to swiftly adopt the EUCS and resolve the political deadlock by not conflating legal and cybersecurity considerations in a technical instrument[4]. In spite of the numerous concerns raised, two years later, the latest draft still presents numerous challenges and questions that ENISA should clarify before the ECCG can consider to approve the EUCS as a candidate scheme to be handed over formally to the European Commission. It is crucial that policymakers take our suggestions and amendments into consideration. In particular, they must further explain how the different levels of assurance will impact workloads and critical entities that will use cloud services, as well as the reasoning for applying different levels of assurance.

[4] Some of these stakeholders include: EACH (https://eachccp.eu/wp-content/uploads/2022/08/EACH-Letter-Cybersecurity-Certification-Scheme-for-Cloud-Services-August-2022-2.pdf) and BDI (https://english.bdi.eu/media/publications/#/publication/news/european-cybersecurity-certification-scheme-for-cloud-services-eucs/)