European Cybersecurity Certification Scheme for Cloud Services

Brussels, 14 June 2022 - Our organisations are closely following the work related to the Cybersecurity Certification Scheme for Cloud Services (EUCS) being undertaken by the European Union Agency for Cybersecurity (ENISA). The companies we represent support the EU's ambitions to tackle global cyber threats and protect citizens, institutions and businesses through cybersecurity certifications. However, as ENISA prepares to finalise the EUCS, we would like to express our concerns about several of its procedural and substantial elements. In particular, the potential inclusion of unhelpful 'digital sovereignty' requirements risks negatively impacting both European organisations that provide cloud computing solutions and those ones that use them and require a high-level of cybersecurity assurance.

Our concerns include:

- There's been limited transparency and lack of stakeholder engagement that have characterised EUCS discussions throughout the scheme's development. The role of stakeholders, including industry, and the reliance on consensus-based international standards are vital to ensuring that cybersecurity requirements are effective.

- The proposed 'digital sovereignty' requirements, regardless of the assurance level for which they are aimed at, are purely politically motivated, will create complex legal compliance and will not add to increased levels of cybersecurity. The EUCS is foreseen in the Cybersecurity Act as a technical instrument and should not be compromised by consideration that are political in nature.

- The potential inclusion of provisions would require the maintenance, operations of the cloud service, and data to be solely located within the EU would limit cloud service providers' eligibility to the EUCS. This would create obstacles to information sharing between organisations, which is an essential tool for reducing cybersecurity risk. Data localisation requirements, in particular, would also increase the costs of maintaining state-of-the-art solutions and reduce alternative storage in cases of data losses or network outages.

- The proposed requirements, particularly the proposed ownership requisites, will create significant entry barriers for non-EU headquartered companies and EU companies with international or global operations. This will limit competition in the cloud market, raise costs and reduce the selection of trusted technology partners for European businesses, ultimately hindering innovation and digital transformation capacities in the EU.

- The current European cloud market capacity cannot sustain the needs of EU demand, both in terms of quantity and quality. Hence, introducing these requirements will determine users' reliance on the limited number of providers offering adequate services, resulting in a risk of 'reversed concentration'. This would dramatically impact customers' ability to select the technology and cloud service providers that best meet their operational needs.

- EU Members States are not in unanimous agreement about introducing these requirements in cybersecurity certification schemes. Several countries are signalling their support for discussing,

defining and clarifying a common position on sovereignty at the political level, instead of introducing these requisites in the EUCS. Such lack of agreement among Member States may fragment the Single Market, reduce trust and increase compliance costs for industry.

Based on the above, we urge ENISA and the European Commission to inform stakeholders of the state of the discussion and engage with them throughout the finalisation process to ensure that the EUCS does not include unnecessary and discriminatory requirements.

Signatories:

- American Chamber of Commerce to the European Union (AmCham EU)
- BSA | The Software Alliance
- Computer & Communications Industry Association (CCIA Europe)
- The Information Technology Industry Council (ITI)