U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

October 31, 2023

Mr. Juhan Lepassaar
Executive Director
European Union Agency for Cybersecurity
Ethnikis Antistaseos 72 & Agamemnonos 14
Chalandri 15231, Attiki
Greece

Re: U.S. Chamber of Commerce comments regarding the European cybersecurity certification scheme (EUCC) for ICT products

Dear Mr. Lepassaar:

The U.S. Chamber of Commerce ("U.S. Chamber") welcomes the opportunity to provide feedback to the European Commission's public consultation on the Draft Implementing Act laying down rules for the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC).

The U.S. Chamber, as the world's preeminent business advocacy organization, champions free enterprise and facilitates American trade and investment globally. Within Europe, our affiliations run deep. We collaborate extensively with AmCham EU and American Chambers of Commerce across all 27 Member States. We maintain a close relationship with our colleagues at BusinessEurope, among other Member State business associations.

The U.S. Chamber believes cybersecurity certifications, such as those authorized in the Cybersecurity Act, Regulation (EU) 2019/881 of the European Parliament and the Council, are an important tool in a broader risk management program for enhancing trust and security in connected products, services, and processes. Our members leverage numerous international standards, certifications, and frameworks to manufacture products that are more secure and more resilient by design. From a global perspective, cybersecurity certification and standards-based attestation can be critical to creative opportunities for harmonization and mutual recognition.

The candidate EUCC scheme is risk-based, grounded in technical standards, and envisions a robust cybersecurity baseline for certified products. The U.S. has assessed the EUCC's foundational guidelines and anticipated implications. As representatives of U.S. business, we recognize the EUCC's pivotal role in standardizing cybersecurity certifications across Member States, thus fostering trust in ICT products. In particular, we welcome the lack of any "sovereignty" requirements included in the draft scheme, which we believe respects the primary objective of the cybersecurity certification schemes envisioned in the Cybersecurity Act. The U.S. Chamber supports the fact that the EUCC will supersede any existing national cybersecurity certification scheme, enabling much-needed harmonization at the EU level, which will have a considerable impact on the global ICT ecosystem, including U.S. stakeholders.

## 1. Outcome Focused, Risk-Based, Consensus Standards Are Critical for Driving Regulatory Cohesion

Consistent with the security objectives of Article 51 of the 2019 Cybersecurity Act, the U.S. Chamber believes that any candidate cybersecurity certification scheme should be aligned with technical, consensus, international information security standards, non-discriminatory to foreign suppliers, and technology neutral.

Article 51 | Security objectives of European cybersecurity certification schemes

(a) to protect stored, transmitted, or otherwise processed data against accidental or unauthorized storage, processing, access, or disclosure during the entire life cycle of the ICT product, ICT service, or ICT process;
(b) to protect stored, transmitted or otherwise processed data against accidental or unauthorised destruction, loss or alteration or lack of availability during the entire life cycle of the ICT product, ICT service or ICT process;
(c) that authorized persons, programs, or machines are able only to access the data, services, or functions to which their access rights refer;
(d) to identify and document known dependencies and vulnerabilities;
(e) to record which data, services, or functions have been accessed, used, or otherwise processed, at what times, and by whom;
(f) to make it possible to check which data, services or functions have been accessed, used or otherwise processed, at what times and by whom;
(g) to verify that ICT products, ICT services and ICT processes do not contain known vulnerabilities;
(h) to restore the availability and access to data, services, and functions in a timely manner in the event of a physical or technical incident;
(i) that ICT products, ICT services and ICT processes are secure by default and by design;
(j) that ICT products, ICT services, and ICT processes are provided with up-to-date software and hardware that do not contain publicly known vulnerabilities and are provided with mechanisms for secure updates.

Meeting the above-mentioned security objectives for European cybersecurity certification schemes is best done using outcome-focused, risk-based, consensus standards that reflect global best practices developed with industry, regulators, academia, civil society, and government. Internationally recognized standards development organizations (SDO) promulgate consensus standards based on technical merit and not based on nationality, employer, or person originating them. They enable safe, secure, reliable, and interoperable global technology, products, and processes. Regulator's use of outcome-focused, risk-based, technical consensus standards will simplify compliance, enhance cyber resilience, scale globally, and adapt to emerging threats and new technologies.

## 2. Duplication and Mutual Recognition

A significant challenge is the looming prospect of duplicative cybersecurity certification schemes between the EU and the U.S. The U.S. recently introduced the Cyber Trust Mark (see White House Fact Sheet), and the Federal Communications Commission has opened a public consultation on the program. In addition, the U.S. Department of Energy announced that it would begin a new initiative to research and develop cybersecurity labeling for energy products. The forthcoming Cyber Resilience Act (CRA) is envisioned to require cybersecurity certification for specific products. We are concerned that there will be overlap and duplication between CRA certifications and those covered by the EUCC scheme. The EUCC scheme should only cover products already covered by the SOG-IS scheme rather than a broader suite of ICT products, services, and processes.

This redundancy compounds operational challenges and could hinder the timely introduction of groundbreaking solutions. The U.S. Chamber strongly endorses a mutual recognition framework between the EUCC and the U.S. Common Criteria spanning all levels (EAL1-EAL7).

The U.S. Chamber is pursuing a cohesive regulatory framework that enables compliance activities that can be performed once and recognized multiple times by different regulators in different jurisdictions without customization. Such a coherent regulatory regime reduces the resources an organization must expend or divert to cybersecurity compliance, allowing it to invest those resources in cyber risk management programs. What is critical for the success of these cybersecurity certification schemes to realize their potential and market penetration is (1) alignment with technical consensus standards and (2) mutual recognition programs that enable certifiers to leverage and scale cybersecurity certifications at home and abroad. For example, products certified to ETSI 303.645 or ISA-62443 should be recognized in European and U.S. marketplaces as having met recognized standards for cybersecurity.

3. Assurance levels of European Common Criteria-based cybersecurity certification scheme (EUCC).

Article 52 of the Cybersecurity Act provides three assurance levels for cyber certification of products, services, and processes in European schemes, including basic, substantial, and high. Security requirements corresponding to each assurance level would be commensurate with the risk associated with the intended use of the product and the probability and impact of an incident. The proposed EUCC Implementing Act does not allow products to be self-certified at a basic level of assurance. We recommend that a basic assurance level be added to the scheme.

4. Conformity Self-Assessment

Consistent with Article 53 of the Cybersecurity Act regarding conformity self-assessment, the U.S. Chamber supports the responsibility of a manufacturer or provider of an ICT product, service, and process to issue an EU statement of conformity stating that a product fulfills the security objectives outlined in the scheme. To facilitate the market uptake of the EUCC scheme, the U.S. Chamber proposes that conformity self-assessment be extended to include products evaluated at the substantial level. This measure promises streamlined certification, favoring both industry and consumers.

5. Unified Rules and Validity Variance

Harmonized rules for coordinated vulnerability disclosure requirements are critical, and steps must be taken to align European Union rules for manufacturers of products with digital elements. We ask that ENISA and the Commission champion coordinated legislation, aligning vulnerability management with established acts like NIS2 and the forthcoming Cyber Resilience Act. The U.S. Chamber strongly believes that required vulnerability reporting obligations should only apply to patched vulnerabilities that have been actively exploited and pose a significant cybersecurity risk. Public disclosure of unmitigated, potentially exploitable vulnerabilities creates substantial risk for users. The candidate EUCC, the NIS2, the Cybersecurity Act, and the future Cyber Resilience Act must keep the reporting lines for vulnerabilities and require reporting to agencies to mitigate vulnerabilities only within 72 hours of effective mitigations or patching becoming publicly available.

Furthermore, clarity in EUCC certification duration, be it a consistent term like five years or discretion vested in each Member State's National Cybersecurity Certification Authority (NCCA), is crucial.

6. Voluntary

The U.S. Chamber recognizes the voluntary nature of the EUCC scheme for all assurance levels. It supports the voluntary use of the scheme and EU statement of conformity unless otherwise specified in Union or Member State Law. Voluntary cybersecurity certification will ensure speedy and efficient use by the market. Voluntary schemes allow for flexibility in the market. They encourage innovation by providing a framework companies can voluntarily adhere to without imposing rigid requirements. This flexibility can be particularly beneficial in the rapidly evolving field of technology, allowing companies to adapt and innovate without being constrained by strict mandatory regulations. Voluntary schemes are often more readily accepted by companies. When companies willingly participate in certification programs, it tends to promote a culture of security-conscious development. It also encourages market adoption as companies see the benefit of distinguishing their products through certification, signaling to consumers that their products meet specific cybersecurity standards.

7. Collaboration Gap and Expert Engagement

The U.S. Chamber underscores the importance of public-private collaboration between industry and public sector bodies in developing European Cybersecurity Certification schemes. We note the absence of consultations with the Stakeholder Cybersecurity Certification Group (SCCG) from recent drafts of the EUCC scheme. The regular interface between the European Cybersecurity Certification Group (ECCG) and SCCG is essential to harness industry expertise in EUCC's deployment.

###

In conclusion, while the U.S. Chamber acknowledges the Union's strides in crafting a harmonized cybersecurity certification framework across the single market, we advocate for a synergistic approach with the U.S. and EU. Addressing our outlined concerns will not only propel business on both sides of the Atlantic but also amplify the worldwide cybersecurity framework. Thank you for considering our views; the U.S. Chamber stands ready to engage with the Commission further and constructively on this important matter.

Sincerely,

Vincent M Voci

Vincent M. Voci
Vice President, Cyber Policy and Operations
U.S. Chamber of Commerce

Marjorie Chorlins

Marjorie Chorlins
Senior Vice President, Europe
U.S. Chamber of Commerce