Position Paper

SEIZING THE OPPORTUNITY: TIC COUNCIL RECOMMENDATIONS FOR AN AMBITIOUS CYBERSECURITY ACT REVISION

June 2025

INTRODUCTION

TIC Council, the international trade association representing the independent testing, inspection, and certification (TIC) sector, welcomes the European Commission's commitment to strengthening cybersecurity governance across the EU. Safeguarding citizens' privacy, ensuring businesses can conduct operations without disruption, and protecting critical infrastructure from cyber threats are essential to fostering economic growth and building public trust in an increasingly digital and interconnected world.

Adopted in 2019, the Cybersecurity Act (CSA)[1] serves as a cornerstone of the EU's cybersecurity framework. It not only provides the legal mandate for the European Union Agency for Cybersecurity (ENISA) but also establishes the European Cybersecurity Certification Framework (ECCF), aimed at improving the security of ICT products, services, and systems through EU-wide certification schemes.

TIC Council Members play a central role in the effective implementation of the CSA and the functioning of schemes such as the EU Common Criteria (EUCC)[2], as well as those currently under development, including EU5G and EU Cloud Services (EUCS). As accredited Conformity Assessment Bodies (CABs)[3], our Members play a key role in enabling industry to obtain EU cybersecurity certifications, while our technical experts contribute to the design of certification schemes and complementary standardisation efforts.

TIC Council believes that the ongoing revision of the Cybersecurity Act (CSA) is a timely opportunity to fully realise the ambitions of the original legislation and ensure it is fit for today's evolving digital landscape and cybersecurity threats. The revision should prioritise greater legal clarity, including a clear definition of how the CSA interacts with other key EU cybersecurity legislation—such as the NIS2 Directive[4] and the Cyber Resilience Act (CRA)[5]—to provide coherence and predictability for the market. It should also streamline reporting obligations and reinforce efforts to reduce cybersecurity risks in a way that supports Europe's digital resilience and global competitiveness.

---

[1] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

[2] Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC).

[3] Becoming a CAB, European Union Agency for Cybersecurity (ENISA), https://certification.enisa.europa.eu/browse-topic/becoming-cab_en.

[4] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

[5] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act).

To this end, TIC Council puts forward the following recommendations for consideration in the CSA revision.

RECOMMENDATIONS

1. Need to strengthen stakeholder input to fully realise the potential of the CSA:

- The ambitions of the CSA have not yet been fully achieved. To date, only one certification scheme has been adopted (EUCC), while others remain stalled in the development phase. This underscores the need for greater agility, efficiency, and responsiveness within the EU cybersecurity certification framework for key stakeholder opinions to be taken into consideration, particularly through the Stakeholder Cybersecurity Certification Group (SCCG). In parallel, fostering closer cooperation between the SCCG and the European Cybersecurity Certification Group (ECCG) could help accelerate progress in coordinating views.
- Cooperation and regular exchanges with the ECCG are especially relevant as legislation such as the NIS 2 Directive is being implemented differently across Member States. The involvement of national authorities—such as accreditation bodies, notifying authorities, and market surveillance authorities—is critical for the accreditation of CABs for schemes such as the EUCC. Ensuring these authorities are meaningfully engaged with private stakeholders and the broader cybersecurity industry is therefore essential.
- The European Commission, ENISA, and Member States should also encourage activities such as regular roundtable discussions that bring together key actors across the cybersecurity ecosystem—from TIC companies to manufacturers and the broader quality infrastructure community. This would promote better coordination, shared understanding, and faster development of effective certification schemes.

2. Develop new and targeted European Cybersecurity Certification schemes:

- To ensure a strengthened relevance and effectiveness of the CSA, the development of new and targeted European Cybersecurity Certification schemes is essential. Current gaps in the EU cybersecurity framework must be addressed to provide comprehensive and future-proof coverage. To guarantee the EU remains cyber-resilient and, in turn, safeguards and reinforces its global competitiveness, the TIC sector strongly supports the expansion of the cybersecurity certification landscape in the following key areas:
    1. Managed Security Services (MSS);
    2. Consumer IoT products;
    3. AI systems and products with embeded-AI;
    4. Supply chain cybersecurity;
    5. Space systems and equipment;
    6. Dual-use technologies;
    7. Quantum computing and post-quantum cryptography (PQC).
- These domains are critical for enhancing Europe's cybersecurity resilience. For instance, a dedicated scheme for consumer IoT products could support compliance with the CRA, while a scheme for AI systems would

align with the AI Act[6], and for space systems and equipment could help address cybersecurity requirements under the forthcoming EU Space Law. All of these schemes would serve as valuable tools to support and align with the European Commission's goals of streamlining compliance processes. They would enable manufacturers to demonstrate conformity with the requirements of EU legislation through voluntary certification, while also ensuring the safety and security of products and services placed on the EU market.

- Similarly, developing a certification scheme for quantum computing and PQC is essential to position the EU as a global leader in this strategic field, especially in light of the upcoming Quantum Act planned for 2026. As quantum technologies advance, current cryptographic systems risk becoming obsolete, potentially exposing critical infrastructure, communications, and data to severe vulnerabilities. Establishing a PQC-focused scheme now would not only enhance preparedness but also reinforce the EU's strategic autonomy and technological leadership.
- When developing new schemes, we strongly recommend the establishment of clear roadmaps, consultation periods and enhanced transparency across the whole process.
- Lastly, existing cybersecurity standards should be carefully considered when defining the requirements of potential new schemes. TIC Council has actively contributed to strengthening these standards by hosting three cybersecurity hackathons focused on the widely used IoT standard ETSI EN 303 645[7] and CEN-CENELEC EN 18031 series, developed to facilitate compliance with the cybersecurity requirements of the Radio Equipment Directive (RED) Delegated Act[8].

3. Integrate schemes combining multiple requirements:

- New certification schemes should aim to integrate cybersecurity, data protection, and other requirements. This would make them more attractive and useful for manufacturers, while also helping to simplify compliance obligations.

4. Consideration of mandatory certification for certain areas:

- For specific high-risk sectors or products, the introduction of mandatory certification could be considered, provided it is proportionate and risk-based.
- For example, a mandatory scheme for the supply chains of critical entities, such as those covered under the NIS2 Directive, could significantly enhance the resilience of critical infrastructure. We recommend that such

[6] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

[7] TIC Council Cybersecurity Hackathons – Strengthening ETSI EN 303 645.

[8] Commission Delegated Regulation (EU) 2022/30 of 29 October 2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive

schemes be built upon well-established international standards like ISO/IEC 27001, SOC 2, and others, where appropriate.

5. Strengthening international cooperation and mutual recognition:

- As cybersecurity is inherently cross-border and ICT products and services are placed on various international markets, aligning certification schemes globally is essential.
- In this context, we strongly encourage the European Commission to pursue, wherever feasible, Mutual Recognition Agreements (MRAs) with third countries. Such agreements would facilitate market access for vendors worldwide while enhancing the overall cybersecurity of products and services.

6. Streamlining reporting obligations, not weakening safety requirements:

- TIC Council supports simplifying and streamlining reporting obligations to reduce administrative burden. However, this must not come at the cost of weakening essential safety and security requirements, which are key to enhancing the EU's cybersecurity resilience and collective protection.

7. Support for policy option 3 – CSA improvements, not repeal:

- Support for policy option 3, which entails targeted legislation to improve and update the CSA. However, we strongly oppose repealing the CSA without a clear and enhanced framework. Any new legislation should complement the CRA and provide a robust foundation for EU cybersecurity.

CONCLUSION

TIC Council and its Members remain available to provide further, more technical feedback on the above-mentioned points and other relevant aspects. As key enablers of Digital Trust, we are committed to engaging with the European Commission and all relevant stakeholders to ensure that the revision of the CSA leads to greater effectiveness and impact across the EU. This will help build a safer, more resilient cyber ecosystem, enhancing the EU's competitiveness and reinforcing citizens' trust in the security and reliability of products and services.

Contact Person
Ángel Moreno Rubio, Digital Policy Manager
Rue du Commerce 20/22, B-1000 Brussels
Tel: +32 487 02 07 32
Email: amorenorubio@tic-council.org

Editor's Note About TIC Council

TIC Council is the global trade association representing the independent third-party Testing, Inspection and Certification (TIC) industry which brings together about 100-member companies and organizations from around the world to speak with one voice. Its members provide services across a wide range of sectors: consumer products, medical devices, petroleum, mining and metals, food, and agriculture among others. Through provision of these services, TIC Council members assure that not only regulatory requirements are met, but also that reliability, economic value, and sustainability are enhanced. TIC Council's members are present in more than 160 countries and the wider TIC sector currently employs more than 1 million people across the globe.