EUROSMART
The Voice of the Digital Security Industry

Eurosmart's Contribution to the Review of the Cybersecurity Act (CSA)

Strengthening ENISA’s role and Improving the ECCF

The European Union is at a critical juncture in shaping its cybersecurity policy and governance. Eurosmart advocates for a more coherent, pragmatic, and effective cybersecurity certification framework. The European Cybersecurity Certification Framework (ECCF), as defined in the Cybersecurity Act (CSA), is already a key element of the European cybersecurity legislative landscape. Even if the effective implementation of the CSA can still be improved, this legislative instrument sets out fundamental and strategic provisions - such as CAB accreditation, NCCA supervision, a peer-review mechanism, and penetration testing for high assurance levels - which should be safeguarded to protect what constitutes European assets in the global cybersecurity race.

Drawing on its active engagement in European cybersecurity policy development, and going beyond the legal revision of the CSA, Eurosmart outlines in this document practical recommendations for enhancing ENISA's mandate, simplifying EU cybersecurity compliance, reinforcing the ECCF, and addressing emerging challenges such as supply chain vulnerabilities and the integration of non-technical requirements. These may include the introduction of data protection principles and qualification processes for specific use cases.

Eurosmart’s approach is not to complicate matters with additional mandatory requirements - which would impose extra burdens on manufacturers - but rather to promote a more agile certification process by reusing existing tools and seeking synergies with other EU cybersecurity-related legislation to facilitate compliance.

Representing the digital security industry in Europe, Eurosmart has been deeply involved in the legislative process of the first version of the CSA. It actively contributed to the adoption of the first EU certification scheme and supported the maintenance of subsequent schemes. The proposals outlined in this document reflect the views of Eurosmart and its members across the various stages of the CSA life cycle. Eurosmart strongly believes that the CSA - particularly the role of ENISA and the functioning of the ECCF - provides real added value to the European digital security ecosystem and actively contributes to the strategic digital autonomy of our continent.

1. Enhancing ENISA's Mandate and Strategic Role

1.2 Central Role in Legislative Interpretation and Compliance Simplification

ENISA should play a central role in interpreting and streamlining the various cybersecurity provisions set out in the EU legislative corpus. As an increasing number of EU legislative instruments—such as the Cyber Resilience Act (CRA), the NIS2 Directive, the EUDI Wallet Regulation, and the AI Act—begin to rely on European cybersecurity certification schemes, ENISA's support becomes indispensable. The agency should focus on identifying overlaps among these instruments and work towards simplifying compliance efforts for stakeholders.

ENISA's mandate should include the publication of structured guidance and materials to enable the reuse of EUCSA certificates as evidence of conformity under other EU laws. This approach should be cost-effective and avoid adding complexity for manufacturers striving to meet essential requirements.

1.3 Supporting Legal Mapping and Market-Oriented Scheme Development

ENISA should also support analytical studies and mappings that demonstrate how existing certification schemes align with legal requirements from various EU regulations. This would contribute to a more coherent and integrated regulatory landscape. When defining new schemes, market-oriented considerations and impact assessments should be conducted. The proliferation of certification schemes is not a desirable outcome; rather, industry would benefit from relying on cross-sectoral schemes or reusing existing building blocks. Development should reflect cost-efficiency and practical implementation needs, while aligning with the timely emergence of relevant technologies. ENISA possesses the technical resources to deliver such assessments, and its support and advisory role to EU legislators would significantly enhance the development, applicability, and uptake of certification schemes across sectors.

1.4 Expansion into New Technical Responsibilities

ENISA should also assume new technical responsibilities. A notable example is the establishment of a European Vulnerability Database, representing a significant step towards a sovereign and independent vulnerability management strategy for the EU. This mission should be formally incorporated into ENISA's mandate.

In addition, ENISA should support the implementation and operation of certification schemes. For example, if widely used critical Free and Open-Source Software (FOSS) lacks proper maintenance by an open-source steward, ENISA could act in this capacity to ensure the security and sustainability of essential digital infrastructure.

1.5 Enhanced Situational Awareness and Technology Dependency Tracking

ENISA's role in situational awareness must also be strengthened. The agency should not only provide relevant technical information but also consolidate recommendations from national cybersecurity agencies to ensure coherent and coordinated guidance across the EU. It should actively identify and highlight critical dependencies on non-EU technologies—including hardware, software, and cloud services—to support risk assessments and strategic planning aligned with both the development of EU cybersecurity legislation and the EU's digital sovereignty objectives.

2. Improving the European Cybersecurity Certification Framework (ECCF)

2.1 Certification as a Legal and Strategic Incentive

From an industry perspective, cybersecurity certification does not necessarily lead to enhanced product security. Instead, it is often pursued to meet market expectations or gain a competitive advantage. To provide meaningful incentives, certification should serve as a mechanism for reducing legal exposure or liability. Cybersecurity certificates that provide a legal presumption of conformity under EU legislation—such as the CRA or NIS2—would be a strong incentive for industry stakeholders.

2.2 Recognition as Due Diligence Evidence

From a liability standpoint, EU cybersecurity certificates should be recognised as legitimate tools for manufacturers to demonstrate due diligence, comparable to the function currently performed by harmonised standards. This would provide legal clarity and support widespread adoption.

2.3 New Certification Schemes for Emerging Technologies

EU Cybersecurity Certification should also address emerging technological domains over the next five to ten years. This includes certifying development processes, such as the Secure Development Lifecycle (SDL), to ensure that organisational practices align with recognised security standards. Dedicated schemes should be developed for complex systems with significant societal impact, including the EUDI Wallet, identity management platforms, and industrial control systems. Certification schemes should also incorporate cutting-edge cryptographic standards, such as post-quantum cryptography. The goal is not to duplicate efforts but to streamline the development of new schemes by reusing existing building blocks wherever possible.

2.4 Lifecycle-Aware Certification Models

There is a pressing need to adopt lifecycle-aware certification models. Products with long operational lifespans—such as those incorporating Qualified Signature Creation Devices (QSCDs)—may remain in use for over a decade. It is unrealistic to expect these products to fully comply with continuously evolving security standards. The ECCF and its associated schemes should therefore accommodate "conditional" certificates that remain valid based on periodic risk assessments, particularly where full compliance is no longer feasible but residual risks are acceptable at high assurance levels.

2.5 Non-technical requirements: Strategic Role in Digital Autonomy and Privacy

Cybersecurity certification should also serve strategic objectives, such as strengthening digital sovereignty. Certification applicants could, for example, opt to receive assurances about immunity from extraterritorial legal obligations or address specific privacy concerns. Optional privacy modules could be introduced at higher assurance levels (e.g. EUCS High+), allowing vendors to voluntarily meet additional requirements based on the nature of the personal data their products process. This would provide proportionate and targeted protection without imposing uniform burdens on all vendors. More broadly, incorporating targeted non-technical requirements into certification schemes can reinforce the EU’s strategic autonomy.

2.6 Formalising Ecosystem-Led Maintenance Model: e.g. ISAC

To ensure the ongoing development and maintenance of certification schemes, ecosystem-led structures should be established to foster collaboration among vendors, laboratories, and national authorities. Information Sharing and Analysis Centre-style forums, such as the EUCC ISAC, should be central to this ecosystem. ISACs are recognised for their agility and trustworthiness, providing a collaborative framework for private-sector input on emerging threats, best practices, and technological innovation.

To strengthen their impact, collaboration between ISACs and relevant subgroups of the European Cybersecurity Certification Group (ECCG) should be institutionalised through structured public-private partnerships (PPPs). This would ensure ISACs play a key role in maintaining and updating certification schemes in line with industry needs and innovation cycles.

3. Simplification and Regulatory Streamlining

3.1 Harmonisation across EU cybersecurity legislatives instruments

The growing complexity of the EU cybersecurity legislative landscape has created significant administrative burdens for industry stakeholders. Varying reporting formats, tools, and compliance requirements across Member States and regulatory instruments present considerable challenges. To mitigate this, the EU should harmonise incident reporting templates and thresholds and standardise reporting timelines and content. A single EU-level reporting platform would help eliminate duplication and streamline compliance.

Cyber risk management requirements should also be unified across all relevant EU laws. ENISA or the European Commission should maintain a publicly accessible matrix mapping obligations under the CRA, NIS2, DORA, and other applicable legislation. This resource would serve as a reference point for manufacturers to identify relevant requirements and determine where obligations overlap.

3.2 Cross-Scheme Recognition to Eliminate Redundancy

The ECCF should further enable cross-scheme recognition—or a "passporting" mechanism—of test and evaluation results. This would prevent redundant assessments, reduce costs, and promote broader industry adoption of certification.

4. Stakeholder Involvement in Scheme Development

4.1. Maintaining an Inclusive Development Model: ENISA's Ad-hoc Working group (AHWG)

The development of effective cybersecurity certification schemes depends on active and meaningful stakeholder engagement. ENISA should continue its central role by convening stakeholders across relevant value chains to develop candidate EU schemes. The existing AHWG model has proven effective and should be retained. Transparent selection processes should ensure contributors are chosen based on technical expertise, geographical representation, and sectoral balance.

4.2. Open Mid-Term Public Consultations

Mid-term development consultations should be conducted through accessible platforms such as GitLab or the ENISA CEF platform to encourage participation and ensure transparency. Feedback received through these channels should be jointly assessed by the ad hoc working groups and the ECCG.

4.3. Transparent Modification Adoption and Maintenance Process

Once ENISA submits a candidate scheme to the European Commission, any subsequent modifications should be reported back to the original working group and clearly explained before adoption into the Implementing Act. The process would then advance to the public “Have Your Say” phase.

The European Cybersecurity Certification Group (ECCG) should be restructured to include formal subgroups responsible for the maintenance of specific certification schemes. The Cybersecurity Act should be updated to reflect this current governance model. These subgroups should be required to publish and maintain annual maintenance roadmaps. The Act should also formalise links with industry-led bodies such as the EUCC ISAC, ideally through privileged or contractual public-private partnerships, to ensure continuous updates and stakeholder engagement.

Conclusion

A revised Cybersecurity Act must support Europe’s ambition for digital strategic autonomy while enabling effective compliance with an evolving cybersecurity regulatory framework. ENISA’s mandate should be strengthened to provide strategic policy input, technical guidance, and a recognised role in the development and maintenance of certification schemes. Its engagement with stakeholders and the wider EU cybersecurity ecosystem should also be formally acknowledged.

The governance of the ECCF should reflect the added value of ECCG subgroups and permit structured partnerships with stakeholder organisations, such as the EUCC ISAC. At the same time, simplifying regulatory requirements and enhancing stakeholder participation will ensure a cybersecurity framework that is responsive, resilient, and aligned with both policy objectives and industry needs. Through these coordinated efforts, the EU can foster a trusted, secure, and sovereign digital environment.

About us

Eurosmart, the Voice of the Digital Security Industry, is a **European non-profit association located in Brussels**, representing the **Digital Security Industry** for multisector applications. **Founded in 1995**, the association is committed to expanding the world's Digital secure devices market, developing smart security standards and continuously improving the quality of security applications.

EUROSMART
The Voice of the Digital Security Industry

Square de Meeûs 35 | 1000 Brussels | Belgium
www.eurosmart.com