EUROSMART
The Voice of the Digital Security Industry

CSA revision – Eurosmart' Answer to the European Commission's call for evidence

Strengthening Strategic Governance, Streamlining Certification, and Safeguarding European Cybersecurity Leadership

Eurosmart, representing the digital security industry in Europe, supports a pragmatic and strategic revision of the Cybersecurity Act (CSA) that strengthens ENISA's role, reinforces the European Cybersecurity Certification Framework (ECCF), and promotes more efficient and agile certification schemes. As the EU digital landscape becomes increasingly complex with instruments such as the Cyber Resilience Act (CRA), NIS2 Directive, and the AI Act, the CSA remains the cornerstone of the European cybersecurity regulatory framework. In this context, synergies should be established to reduce legal redundancy and streamline compliance.

The ECCF, as defined in the CSA, is already a key component of the European cybersecurity legislative architecture. While the implementation of the CSA can still be improved, it provides essential and strategic provisions—such as the accreditation of Conformity Assessment Bodies (CABs), supervision by National Cybersecurity Certification Authorities (NCCAs), a peer-review mechanism, and penetration testing for high assurance levels—which must be preserved to safeguard European assets in the global cybersecurity landscape.

For these reasons, Eurosmart advocates for a more agile approach in revising the Cybersecurity Act, focused on enhancing existing achievements rather than overhauling the framework. A complete reshuffle of this legislative instrument could undermine the rapidly growing ecosystem that supports EU cybersecurity certification.

Therefore, Eurosmart recommends pursuing Option 3, with targeted amendments, as the best path forward to streamline certification processes, schemes' development and reinforce ENISA's role as the EU's cybersecurity agency.

1. Preserving the Foundations of the EU Cybersecurity Certification Framework

To ensure the continued credibility and effectiveness of the European Cybersecurity Certification Framework (ECCF), it is essential to preserve its foundational elements—particularly those applicable to high-assurance levels. These components form the backbone of trust, technical rigor, and institutional reliability that distinguish EU cybersecurity certification globally.

1.1. Penetration Testing for Assurance Level "High"

Penetration testing must remain a mandatory component for assurance level "high" to demonstrate that the ICT products, ICT services or ICT processes correctly implement the necessary security functionalities at the state of the art, and an assessment of their resistance to skilled attackers. Unlike automated "push-button" tests, penetration testing provides critical added value by actively uncovering vulnerabilities under real-world conditions and make sure that products are backdoor safe. This requirement, which should remain under the strict oversight of public authorities, is essential to maintaining the credibility, integrity, and robustness of cybersecurity certifications in Europe. Weakening or removing this obligation would significantly compromise trust in certified solutions and the overall resilience of the European cybersecurity ecosystem. (See Eurosmart position paper).

1.2. Accreditation of Conformity Assessment Bodies (CABs)

Conformity Assessment Bodies must be accredited by National Cybersecurity Certification Authorities (NCCAs), with their activities subject to structured supervision, authorization, and peer review. As the CSA evolves to support multiple certification schemes, it is essential to streamline accreditation processes by aligning or reusing technical and organizational requirements across schemes.

While the CSA and Regulation (EC) No 765/2008 do not mandate the use of ISO/IEC 17065 or 17025, these standards are referenced in the EUCC Implementing Act and are widely recognized in the industry. For greater legal clarity and to ensure consistent quality, these standards should be explicitly referenced in a CSA annex related to CAB accreditation. This would help ensure that only competent and qualified CABs operate within the ECCF.

1.3. Certification Issuance for High Assurance Levels

For cybersecurity certifications at the high assurance level, it is essential that issuance remains the exclusive responsibility of National Cybersecurity Certification Authorities (NCCAs) or Conformity Assessment Bodies (CABs) acting under a formal delegation from these authorities. This governance model ensures that certifications are subject to the highest degree of oversight and public accountability. Allowing only NCCAs, or CABs explicitly mandated by them, to issue high-level certificates guarantees:

- **Consistency and harmonisation** across Member States, reducing the risk of fragmented or uneven implementation of security requirements.

- **Trust and credibility** in the certification process, as public authorities are directly accountable for the endorsement of the evaluation results.
- **Rigorous scrutiny**, including technical evaluations such as penetration testing and source code reviews, is essential for high-stakes applications. Given the critical importance of this process for industry trust and security, it is vital that such evaluations continue to be conducted by a trusted third party.

Delegation to qualified CABs must be governed by clear and transparent criteria, accompanied by regular supervision. The peer review mechanism among NCCAs remains essential to ensure consistency, prevent conflicts of interest, and avoid discrepancies in evaluation quality. The integrity of this model is fundamental to ensuring that high-assurance certifications serve as a trusted benchmark within the EU cybersecurity landscape—both for regulatory compliance and as a signal of trust on the international stage.

2. Scheme Development

Progress in the development of European cybersecurity certification schemes has been relatively slow. While the IoT scheme has been announced, other critical schemes - such as EUCS (for cloud services) and 5G - remain pending, as noted in the Union Rolling Work Programme. It is therefore essential to strike the right balance between agility and the depth of expertise and time needed to develop technically robust and widely accepted schemes.

2.1. Streamlining Scheme Development Through Strategic Focus and Reuse

Eurosmart advocates for an agile and pragmatic approach: rather than multiplying certification schemes, the focus should be on rationalising their number to ensure quality and coherence. Priority should be given to transversal schemes, and to the reuse existing building blocks where appropriate.

In this regard, the EUCC scheme sets a valuable precedent and could serve as a foundational model for the development of future schemes, offering technical methodologies that can be adapted and applied across different technologies and sectors.

2.2. Strategic Approach to Scheme Development

To ensure the timely, efficient, and technically sound development of EU cybersecurity certification schemes, a targeted strategic approach is essential. Eurosmart identifies two key elements in this regard: the central role of ENISA and the importance of properly resourcing the scheme development process.

ENISA's Role: Ensuring Stakeholder-Driven, Sector-Specific Expertise

ENISA should continue to serve as the coordinator and facilitator of scheme development, with a central role in convening stakeholders' representative of specific value chains. The existing Ad Hoc Working Group (AHWG) model for stakeholders' consultation (as set out in Article 48(2) and 58(1)(d)) has demonstrated its effectiveness by bringing together experts with the relevant technical, operational, and sector-specific knowledge necessary to develop robust and

meaningful candidate schemes. This model allows for structured, balanced, and goal-oriented input while maintaining flexibility. It also ensures transparency, geographical diversity, and accountability - key factors in fostering industry's fast adoption and public trust. For the sake of transparency, mid-term development consultations should be conducted through accessible platforms such as GitLab or the ENISA CEF Platform. Feedback received through these channels should be jointly assessed by the ad hoc working groups and the ECCG with the support of the SCCG.

Finally, for the sake of transparency, after ENISA submits a candidate certification scheme, any changes before its formal adoption should be transparently communicated to the original HAWG and discussed before entering the public "Have Your Say" phase.

Resource Allocation: Empowering ENISA to Develop Schemes

To sustain and accelerate this expert-driven process, additional resources should be allocated to ENISA. This includes funding and staffing to support the coordination of multiple AHWGs, the provision of technical studies, legal mapping (e.g.: cybersecurity requirements in different pieces of EU legislation), and the publication of guidance materials. Adequate resourcing will ensure that scheme development timelines align with policy demands and market needs, avoiding unnecessary delays that could hinder uptake or compliance with other EU regulations such as CRA, NIS2, or DORA.

Moreover, while the European Standardisation Organisations (ESOs) play an important role in the broader standardisation ecosystem, their open and consensus-based processes are not well-suited to the development of cybersecurity certification schemes. The absence of contributor selection mechanisms can lead to unstructured participation, slower progress, and inconsistent outputs. Additionally, the level of expertise within ESO processes may not always align with the technical depth required for high-assurance evaluations.

In contrast, ENISA's Ad Hoc Working Group (AHWG) model ensures that only qualified and relevant experts—including national authorities, industry stakeholders, Conformity Assessment Bodies (CABs), testing laboratories, and academia—are involved in shaping certification schemes. This targeted, expert-driven approach helps align scheme development with both regulatory objectives and market implementation needs.

3. Integrating Non-Technical Requirements to Support Strategic Objectives

3.1. Immunity and privacy requirements

Cybersecurity certification should not only serve technical assurance goals but also support the EU's broader strategic priorities, including digital sovereignty and the protection of fundamental rights. To this end, EUCSA schemes should incorporate targeted and voluntary non-technical requirements, particularly at higher assurance levels. For example, under a proposed EUCS "High+" level, certificate applicants could opt to demonstrate immunity from non-EU legislation that may compel the disclosure of personal or sensitive EU data. Similarly, enhanced privacy requirements - such as mandatory GDPR compliance and potentially extending data protection obligations - would reinforce the protection of user data without imposing additional burden on all vendors.

Such non-technical requirements should be enabled **as optional modules for specific assurance levels**, enabling vendors to tailor their compliance to the nature and sensitivity of their products or services (e.g.: according to the nature of the personal data the product/service processes). This proportionate and flexible approach would enhance trust while avoiding unnecessary burdens.

In addition, EUCSA schemes should align with non-technical obligations arising from other EU regulations such as DORA, NIS2, and the AI Act, to ensure coherence across the regulatory landscape.

3.2. Qualification process

A defined qualification process should be introduced in the CSA to identify which services or organisations are eligible for certification under these enhanced criteria. This process would involve:

- **Evaluation** by NCCA-accredited laboratories,
- **Validation** by NCCAs based on audit results, and
- **Ongoing maintenance** through annual audits and continuous compliance monitoring.

By integrating these strategic elements, EU cybersecurity certification can become a more effective instrument for reinforcing Europe's digital autonomy and ensuring a high level of trust and accountability in certified products and services.

4. Scheme Maintenance: Leveraging Public-Private Partnerships

The long-term success and credibility of EU cybersecurity certification schemes depend not only on robust initial development but also on their ongoing maintenance. To ensure schemes remain technically relevant, aligned with emerging threats, and reflective of market evolution, the European Cybersecurity Certification Group (ECCG) and its schemes' dedicated subgroups must work closely with stakeholders from across the cybersecurity ecosystem. A structured public-private partnership (PPP) model, anchored in collaboration between public authorities and industry experts, should be institutionalised as part of the Cybersecurity Act (CSA) revision.

Technical documents - such as interpretation guidelines and state-of-the-art references - are essential to support the ongoing maintenance and implementation of certification schemes. Their development may require collaborative drafting and editorial support from the broader European cybersecurity ecosystem.

The EUCC ISAC (Information Sharing and Analysis Centre) provides a proven, agile model for such collaboration. It demonstrates the value of trusted, structured input from industry, labs, and national authorities, and should serve as a blueprint for future scheme maintenance efforts. Eurosmart advocates for a two-step maintenance approach:

4.1. ECCG Subgroups – Formalising Public Oversight

To institutionalise scheme maintenance, dedicated ECCG subgroups should be formally established by the CSA for each certification scheme and co-led by the European Commission and ENISA. These subgroups would:

- **Be composed of representatives from** Member States, particularly NCCA's experts, ensuring public oversight and readyness for legal endorsement of maintenance documents that should be incoporated in the Scheme's implementing act.
- **Be responsible for the** technical maintenance and prepare the scheme updates, reflecting evolving standards, interpretation methodology, attack methods, and regulatory needs.
- **Be mandated by the CSA to** prepare and publish annual maintenance roadmaps, in close consultation with relevant stakeholders. These roadmaps would define the planned updates, documents to be revised, and areas requiring clarification or extension—ensuring transparency and predictability for industry participants.

4.2. ISAC – Embedding EU cybersecurity Ecosystem-led Technical Expertise

In parallel with the formalisation of ECCG subgroups, Information Sharing and Analysis Centres (ISACs)—such as the EUCC ISAC—should be recognised as the technical arm of the maintenance process, bringing together key stakeholders from across the EU cybersecurity landscape. ISACs are valued for their agility, neutrality, and technical credibility, offering a collaborative framework for private-sector contributions to critical elements such as scheme interpretation, evaluation methodologies, attack paths, and threat modelling.

These trusted forums gather a wide range of actors, including vendors, testing laboratories, Conformity Assessment Bodies (CABs), National Cybersecurity Certification Authorities (NCCAs), National Accreditation Bodies (NABs), and other relevant experts who:

- **Prepare maintenance documents** with market-driven insights, technological foresight, and operational feedback;
- **Select qualified experts** across the cybersecurity value chain using a FRAND (Fair, Reasonable, and Non-Discriminatory) approach;
- **Respond to emerging vulnerabilities** and address implementation challenges in a timely manner to maintain the scheme at the State-of-the-Art;
- Help ensure that **certification schemes remain** technically relevant, practically implementable, and aligned with evolving market and policy needs.

To strengthen this collaboration, the CSA should formalise the possibility for the ECCG subgroups to officialise strong liaisons **contractual Public-Private partnerships (cPPPs)** that would allow an official recognition and increase the attractivity of this stakeholders' structure. For example, the EUCC ISAC Steering Committee, comprising NCCAs and designated stakeholder representatives, could be officially recognised as part of the EUCC scheme's governance and maintenance structure.

5. 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.

Moreover, as laid down in Article 55 of the Cybersecurity Act, the manufacturer or provider of certified ICT products, services, or processes is required to inform the National Cybersecurity Certification Authority (NCCA) of any disclosed vulnerabilities. When such a vulnerability arises, the ISAC can serve as a trusted forum for discussion, bringing together NCCAs, ITSEFs, laboratories, affected vendors, and the product issuer to jointly conduct a risk assessment and coordinate appropriate communication. This collaborative environment facilitates efficient information exchange among stakeholders and helps ensure that accurate, timely, and consistent messages are conveyed to relevant parties

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