Connect Europe & GSMA views on the Cybersecurity Act Review

June 2025

Section 1: Mandate of ENISA

Connect Europe and GSMA welcome the opportunity to comment on ENISA's mandate and to share our views on its future mandate and prioritization of tasks.

Our members support the continuation of ENISA's mandate and its strengthening to facilitate harmonization, simplification and a common understanding of the cybersecurity landscape. This could be achieved particularly by increasing ENISA's ability to provide guidance and support regarding technical measures, and by ensuring ENISA has adequate resources to perform its current and future tasks.

To prevent fragmentation in cybersecurity initiatives and existing frameworks, ENISA's mandate should explicitly list further tasks to support simplification and further harmonisation using best practices across the EU. These tasks include the following:

- To support compliance efforts, ENISA should conduct a comprehensive analysis and mapping exercise, based on international standards, to identify which standards meet security requirements under various regulations, highlight gaps, identify where regulatory fragmentation exists, and recommend any additional measures to simplify and harmonise, using a risk-based approach. International standards should be the foundation for compliance, and the mapping exercise should clearly show the interplay between EU and international standards. To complement this, ENISA should create a centralised repository and provide guidance to national authorities and regulated entities on the standards to use for compliance.
- ENISA should have a stronger role in the development of standards, and its mandate should be expanded to include active participation within the European and International Standardization Organizations[1] – particularly in light of the forthcoming standards under the Cyber Resilience Act (CRA). ENISA's participation in standardisation bodies would support the timely development of security standards in close collaboration with private stakeholders. Harmonised standards should remain the preferred approach, while reliance on common specifications for compliance demonstration must be limited to narrowly defined and well-justified cases—such as when standardisation requests are rejected.
- ENISA should always provide concrete dates by which advice and technical guidelines should be completed (whether by EU working groups or national technical authorities). Without clear and harmonised timelines and sufficient time to prepare for new requirements, companies risk operational disruption, compliance gaps, and unnecessary costs. Predictable timelines enable better project planning, budgeting, and sustainable security improvements.
- In its annual report ENISA should report on the progress of cyber security best practices at the European level, simplification initiatives (e.g. single point of contact, incident reporting), cooperation between designated authorities, harmonisation and remaining gaps, and suggest

[1] As highlighted by the Council conclusions on ENISA (paragraph 26)

improvements.

- ENISA should play a key role in developing technical best-practice guidelines that integrate all Member State practices on the "once-only" principle/centralisation of security incident management. Multiple EU laws require telecommunications and digital service providers to report security incidents and vulnerabilities. However, inconsistent procedures, thresholds, and designated authorities across these frameworks lead to duplicated efforts. To reduce administrative burdens and enhance the efficiency of security incident management ENISA should develop guidelines and practical support such as harmonised templates for incident reporting.
- In the interest of improving communication with stakeholders, ENISA should play a role in convening National Technical Authorities (NTAs), CERTs and industry on a pan-EU basis to share intelligence/threat insights, in addition to existing mechanisms at national level. Such a dialogue could help shape ENISA's early warning mechanisms and resilience frameworks, support capacity building, allow for dialogue on relevant topics like certification, and establish a platform for exchange on best practices, allowing for more direct and regular contact with relevant stakeholders in an area that is often time sensitive and requires swift action.
- ENISA should be tasked by the European Commission to evaluate and provide recommendations on Cyber Security Rating. Currently, EU companies are often cyber-rated by international rating agencies without transparent and/or appropriate cyber rating methodologies. This can have detrimental effects on the rated companies. We believe the EU should establish clear rules governing the operations of Cyber Rating Agencies within its jurisdiction, ensuring transparency and appropriateness of methodologies and EU-level oversight. To achieve this, a comprehensive debate should be initiated, involving consultation with all relevant stakeholders, with the aim of defining minimum requirements and procedures for compliance assessment[2].

Section 2: European Cybersecurity Certification Framework

Our members support voluntary EU wide cybersecurity certification schemes, as they have significant potential to demonstrate regulatory compliance within the evolving and increasingly complex regulatory landscape. They can also help establish presumptions of conformity with some requirements under EU cybersecurity regulations (e.g. the NIS2 Directive, DORA, the CRA, etc.). Harmonising cyber security requirements across markets and reducing administrative costs associated with market fragmentation, caused by differing national certification schemes and inconsistent regulatory obligations, is crucial, particularly for multi-country organisations. Europe-wide schemes could help achieve this objective.

European cybersecurity certification schemes should be firmly grounded in international standards to maximise their relevance and acceptance in global markets, including those beyond the EU. This is also particularly relevant in the context of global supply chains. Additionally, accompanying guidance should be made available well before EU schemes become applicable to enhance the schemes' effectiveness and provide greater certainty of compliance for certified organisations. The schemes should be mapped against the products, services and processes they are designed to apply to,

[2] For more information:
Cyber Security Rating – a rising challenge for EU industries, Connect Europe (March 2025);
Cyber Risk Quantification and Cyber Security Rating: What About Mobile Telecommunications Service Providers?, GSMA (August 2024).

including relevant standards and the interplay with relevant security legislation.

It should be noted that it remains unclear how the EU Cybersecurity Certification Scheme on Common Criteria (EUCC) is going to be used in practice, and other relevant schemes, such as the one for 5G, are still under development. As a result, the actual benefits of the European Cybersecurity Certification Framework (ECCF) for the market remain largely untested. However, the experience of companies facing significant overhead when seeking to obtain the EUCC should be taken seriously. For EU cybersecurity certification to achieve widespread adoption, associated costs must be kept manageable.

Looking ahead to the future ECCF, European certification schemes should be market-driven, remain flexible to respond to evolving technological trend and therefore remain voluntary. Before deciding whether a scheme should be made mandatory, such a decision should be preceded by a robust and transparent process. The Commission should provide strong justification that mandatory certification is the most effective and efficient means for private companies to increase cybersecurity across the EU. Furthermore, the assessment should be subject to a thorough and timely public consultation involving all relevant stakeholders, and particularly the 'risk owners' from industry.

To incentivize the adoption of cybersecurity certifications without placing excessive financial burdens on companies, any Member State policy providing financial support for certification-related costs should be designed to minimise administrative and legal burdens. In particular, such policies could take the form of general measures accessible to all relevant undertakings. Special attention should be given where a Member State has made certification mandatory for certain products, services, or users, as this may justify targeted support schemes.

To simplify processes in supply chain management a once-only principle should be applied to certification. For ICT products, services, or processes, which form part of a regulated ecosystem – for example digital infrastructure (regulated under NIS2) or services to financial entities (regulated under DORA) – if certified under a European certification scheme, no additional evidence or audits should be required for the same certified service/product/process in order to demonstrate compliance with legislation.

Regarding the process of developing and adopting certification schemes under the CSA, our assessment is rather negative. The timeline and transparency of the process are highly unsatisfactory. As evidence of this, five years after the establishment of the ECCF, only one relevant scheme has been introduced to the market and with limited use in the market. Others have stalled in an opaque process where the roles and responsibilities of the involved parties, identified issues, the state of play and next steps remain unclear. This situation must change[3].

Connect Europe and GSMA, along with several of our members, have participated in the Stakeholder Cybersecurity Certification Group (SCCG). Our assessment of the SCCG is underwhelming: its role and impact on the certification process are extremely limited. It has largely become a platform for stakeholders to receive periodic updates on the development of schemes and related activities, rather than actively participating in and contributing to the process. The SCCG has had no interaction with the European Cybersecurity Certification Group (ECCG), whose role and responsibilities also remain unclear. Moreover, the flow and format of information shared through the SCCG could be made significantly more accessible.

The roles and responsibilities of both the ECCG and SCCG must be redefined. In particular, the SCCG should evolve into a truly consultative body, with a clear mandate to provide input on draft schemes

[3] As highlighted by the Council conclusions on ENISA (paragraph 7)

that must be genuinely considered in the decision-making process.

Moreover, whilst stipulated in the 2019 CSA Regulation in practice there is a lack of stakeholder involvement in the development of the schemes at working group (WG) level: unless stakeholders have been accepted as member of a specific ad-hoc WG (for which there are not enough places) they have to rely on sporadic updates during events or in media. Instead, ENISA should create a dedicated website for each of the schemes giving regular updates and describing the progress, timeframes and next steps. This should include opportunities to consult beyond just ad-hoc working groups as the draft develops.

To facilitate and expedite the timely delivery of EU certification schemes, ENISA should, upon receiving a request, update, or modification from the Commission, conduct a coherence study with existing schemes and regulations and assess the industrial feasibility of the proposal, following consultations with 'risk owners' and relevant stakeholders. Introducing this new consultation phase would support the development of more realistic, targeted, and timely certification schemes.

Finally, we believe it is not appropriate to introduce requirements under the CSA framework to manage non-technical risks in relation to ICT supply chain security.

Section 3: Simplification of cybersecurity risk-management and incident reporting obligations

There are many areas where cybersecurity requirements and incident reporting obligations can be simplified across the EU evolving regulatory landscape. European telecommunications providers face significant challenges due to overlapping and inconsistent frameworks like NIS2 Directive, DORA, CRA, and the RED Delegated Regulation, to name a few. We welcome the Commission's aim to tackle some of these challenges within the CSA revision, as the impact, overlap and interdependencies of the regulatory regime currently being implemented are not sufficiently clear.

Simplify the legislative ecosystem by removing overlapping and redundant requirements

The regulation of security in electronic communication networks and services is currently fragmented across various EU regulations, creating confusion and inefficiencies. The scope of these regulations is often unclear, resulting in overlapping obligations. A more cohesive regulatory framework is needed to remove overlapping and redundant requirements, streamline compliance and reduce unnecessary complexity.

To illustrate some of this complexity, while the NIS2 Directive primarily addresses providers of critical services, the CRA focuses on digital products; yet both impose requirements for cybersecurity risk-management measures, vulnerability or incident reporting, although with differing standards, platforms, and authorities (a situation also seen with DORA). There is a strong interplay between the supply chain requirements of critical infrastructure providers under NIS2 and the products they use, which are regulated under the RED Delegated Regulation and the CRA. Furthermore, DORA applies to telecom operators in their role as ICT third-party service providers to financial institutions. These differing regulations result in multiple regulators, each with their own requirements and approaches, leading to inefficiencies and increased time and cost burdens.

The revised CSA should aid in simplifying this complex landscape, rather than adding to it. To ensure coherence and reduce unnecessary complexity, provisions in vertical or sector-specific legislation should be repealed when the same issues are already covered by similar obligations in horizontal

regulation. Where other legislation imposes cybersecurity obligations on digital service providers already covered by NIS2, compliance with NIS2 should be presumed sufficient. For example, if sector-specific regulations such as DORA require secure and resilient services, no additional audits or regulatory requirements should be imposed on entities already compliant with NIS2.

Provide timely, guidance based on international standards

A common approach to security regulation would simplify the current complex landscape. All security legislation should be accompanied by guidance on how to comply with security requirements at least 24 months before the legislation takes effect, with the presumption that following this guidance ensures product or service compliance. Without this, companies risk operational disruption, compliance gaps, and unnecessary costs. Additionally, all new regulatory requirements should include a minimum transition period and clearly defined grace periods before enforcement. This would give companies sufficient time to plan, allocate resources, and implement the necessary technical and organisational measures in a structured and sustainable way.

Streamline reporting requirements

Regarding reporting obligations, multiple EU laws currently require telecommunications and digital service providers to report security incidents and vulnerabilities. However, inconsistent procedures, thresholds, and designated authorities across these frameworks lead to duplicated efforts. When revising the Cybersecurity Act and the whole security framework, the European Commission should aim to reduce administrative burdens, foster the use of common standards and enhance the efficiency of security incident management.

Reporting requirements should be simplified and harmonised across regulations, based on best practices, including definitions, what needs to be reported, timelines, thresholds, reporting authorities, and tools (platforms, reporting templates or other). Additionally, establishing a single-entry point for reporting would allow a one-time submission, automatically distributing the information to all relevant authorities. For cross-border incidents or those affecting multiple entities within a group, a single report via the single-entry point of the most relevant jurisdiction should suffice.

Overall, reducing complexity in this area would allow for more resources to focus on incident resolution rather than on reporting. They will also improve awareness of incidents among relevant agencies and provide greater legal certainty for all parties involved through simpler and more consistent legislation. The revision of the CSA should take all these roadblocks duly into account, and should have a clear goal of improving upon the aforementioned points.