Charter of Trust

Contribution to the European Commission Public Consultation on the revision of the Cybersecurity Act

Call for evidence
June 2025

Executive Summary

The Charter of Trust, a coalition of global companies dedicated to cybersecurity, welcomes the opportunity to submit our consolidated response to the European Commission's public consultation on the revision of the Cybersecurity Act. **We endorse policy option 2**, which advocates for targeted regulatory interventions to resolve current issues without adding complexity.

We highlight the need to enhance the role and resourcing of ENISA, the EU's cybersecurity agency, to ensure effective implementation of cybersecurity legislation and the European Cybersecurity Certification Framework (ECCF).

We propose several recommendations, including the introduction of transparent timelines for certification schemes, improved stakeholder engagement, and the establishment of clear communication channels among ENISA, SCCG, and sectoral ISACs.

The Charter calls for a more robust ECCF that includes deadlines for scheme development, greater transparency, and stakeholder consultation. It stresses the importance of aligning certification schemes with international standards to promote global interoperability and reduce compliance burdens. Harmonisation across EU member states and mutual recognition of certifications are also highlighted as critical to reducing regulatory fragmentation. We advocate for technically grounded, standards-based certification schemes and clearer delineation of roles and responsibilities within the certification process. It also seeks clarification on the interaction between voluntary and mandatory certification requirements, particularly in relation to the Cyber Resilience Act (CRA).

To address the growing complexity of incident reporting, we propose a unified, risk-based reporting regime that consolidates obligations under various regulations such as NIS2, CRA, GDPR, and DORA. This would streamline compliance, reduce administrative burdens, and enhance the EU's overall cyber resilience. We also recommend the inclusion of liability protections and grace periods for incident reporting.

Finally, we urge the EU to strengthen supply chain security through a risk-based classification approach and the adoption of baseline cybersecurity requirements for ICT suppliers.

The Charter of Trust reaffirms its commitment to supporting the European Commission in building a secure and resilient digital ecosystem.

Introduction

The Charter of Trust welcomes the opportunity to respond to the European Commission's public consultation on the call for evidence for the revision of the Cybersecurity Act. As a coalition of leading global companies committed to advancing cybersecurity, we aim to provide constructive feedback and recommendations to enhance the effectiveness and implementation of the Cybersecurity Act.

We support **policy option 2**, which allows for targeted regulatory intervention to address existing issues without creating additional complexities. This approach will help address inconsistencies and promote harmonisation between various cybersecurity regulations

The Role of ENISA

ENISA has evolved significantly from a small agency to being recognised both within the EU and globally as the EU's cybersecurity agency. Despite this progress, it has not yet fully realised its potential. We would encourage the Commission to consider the following recommendations:

- It is essential to ensure proper **resourcing** of ENISA to enhance its effectiveness in implementing the ECCF and cybersecurity legislative acts adopted after the Cybersecurity Act. This includes not only financial support but also the provision of necessary personnel, specialised technical expertise, and the budget to ensure the availability and continuous operation of critical services such as the European Vulnerability Database.

- We recommend the introduction of **publicly accessible and regularly updated timelines** for the development and implementation of different certification schemes. This measure would promote transparency and accountability by enabling stakeholders to track progress and evaluate the Commission's adherence to expected milestones, thereby fostering greater trust in the certification process.

- We recommend ENISA to further **foster stakeholder engagement** by engaging the Stakeholder Cybersecurity Certification Group (SCCG) in the certification development process and the development of the Rolling Work Programme for Cybersecurity. Moreover, clear touchpoints and designated points of contact should be established for key industry players and stakeholders (ENISA, SCCG and sectoral ISACs). Institutionalised and targeted communication channels should be created to regularly engage with these stakeholders. Additionally, stakeholders should be provided with opportunities to deepen collaboration with the CSIRTs Network to support information exchange, coordinated incident response, and assistance to Member States during cross-border cybersecurity incidents. A similar approach should be applied within the NIS Cooperation Group to ensure decisions are informed by diverse industry perspectives and practical expertise.

Strengthening the European Cybersecurity Certification Framework - ECCF

The ECCF has a major role in strengthening cybersecurity of our industries, citizens and critical infrastructures against cyber threats by enhancing the security of our ICT supply chains.

The Commission and ENISA can enhance the Certification Framework by implementing the following recommendations:

- **Development and Maintenance of Schemes**: The CSA does not impose any deadlines on bodies involved in creating a cybersecurity certification scheme. As a result, significant time can elapse between the Commission issuing a request to ENISA and the eventual adoption of a new scheme. The **lack of such deadlines** and the associated delay in establishing new schemes not only weakens the credibility of cybersecurity certification of ICT products, services and processes per se, but also brings certainty for the industry.

- **Transparency and Stakeholder Consultation**: Stakeholders and the general public

find it challenging to **access information** about the status of individual cybersecurity schemes. There is a pressing need for greater transparency to build confidence in new schemes. This transparency should allow interested parties to comment on and scrutinise new or amended requirements, especially non-technical ones, and should extend beyond the consultation process. New framework must envisage industry stakeholders' mandate to consult, advise and provide feedback, opinions, assessments to ENISA as well as support market impact assessments related to draft certification schemes. Moreover, European Cybersecurity Certification Group (ECCG) should meet with the SCCG – or a new stakeholder consultation group – on a regular basis to discuss progress and technical issues related to certification schemes.

- **Reference to International Standards**: The EU needs a cybersecurity certification scheme that leverages existing and internationally recognised standards to promote global interoperability and reduce unnecessary compliance burdens for businesses. Draft schemes often **lacked references to international standards or made references to new, unfinished standards**, leading to ambiguous terminology and requirements not grounded in industry best practices. Updates to the Certification Framework should fully ensure the use of existing international standards. Both policymakers and the market would benefit from harmonisation of certification schemes with existing international best practices. By leveraging the international standards in line with Recital 73 of the CSA, ENISA would ensure a quicker and broader market uptake of the schemes and more efficient certification development process. It would also help meet the ambitious legislative agenda and the certification demand.

- **Harmonisation and Mutual Recognition:** To ensure effective and efficient certification across the EU, stronger efforts are needed to harmonise the interpretation and application of certification schemes among national authorities, including accreditation and surveillance practices. Mutual recognition of certifications and conformity assessment frameworks is essential to reduce regulatory fragmentation and ease compliance for companies operating across borders. This includes aligning with international certification schemes and ensuring coherent, harmonised implementation of NIS2 and CRA - particularly regarding certification, incident reporting, supply chain security, and the mutual recognition of the CRA with other international product security programs.

- **Technical-Based Schemes**: A Certification Framework that produces technical, standards-based schemes through open consultations and **reduce vague or overly subjective non-technical criteria** would benefit businesses, citizens, and the European economy. Furthermore, it would reduce uncertainty for Conformity Assessment Bodies and certified organisations and facilitate the approval process. The requirements should be clearly defined, based on a unified risk management framework that addresses the requirements of NIS2, DORA, and CRA, ensuring alignment with GDPR principles where personal data is involved, and auditable with objective criteria to ensure consistency across assessments. The framework should avoid vague or overly subjective non-technical requirements that create uncertainty for CABs and certified organisations.

- **Clarify Roles and Responsibilities within the Certification Process**: There is a need for more precise delineation of roles and responsibilities across all phases of the certification process – from scheme development to implementation, maintenance, and monitoring. This would help avoid overlaps, delays, and inconsistencies in interpretation. A well-defined governance structure should include clear guidance for the interaction between ENISA, national authorities, accreditation bodies, and

Conformity Assessment Bodies (CABs). This could include the requirement for draft schemes to undergo pilot testing by selected CABs and industry representatives to identify practical issues related to auditability, scope, cost and implementation burden, and should be used to fine-tune the certification scheme for real-world conditions.

- **Clarifying Interaction between Voluntary and Mandatory Requirements**: The relationship between voluntary certification schemes under the ECCF and mandatory requirements introduced under the Cyber Resilience Act (CRA) needs to be clarified further. Guidance should be issued on how voluntary schemes can demonstrate compliance with CRA obligations and under what circumstances a voluntary certification may be recognised as supporting or even fulfilling CRA requirements. This is essential to avoid confusion and ensure alignment between regulatory instruments. This said, **CSA should keep voluntary nature of cybersecurity certification schemes**.

Simplification agenda

The revision should aim to streamline reporting obligations to reduce overlaps and administrative burdens on businesses. Clear and concise reporting requirements will facilitate compliance and improve overall cybersecurity resilience.

- **Harmonised and simplified incident reporting:** The Commission's objective to address the complexity in cybersecurity reporting through the Digital Simplification Package is critical. The multiple incident reporting regimes required by the General Data Protection Regulation (GDPR), Network and Information Systems Directive 2 (NIS2), the NIS2 Implementing Regulation, the Cyber Resilience Act (CRA), and the Digital Operational Resilience Act (DORA) have varying thresholds, timelines and content requirements, are resulting in inconsistent and duplicative incident reporting requirements. These divergences impose unnecessary burdens on businesses and hinder effective incident response.

- The growing complexity in incident reporting can ultimately **cause companies to divert crucial cybersecurity resources away from mitigation, response, and recovery efforts** toward managing compliance obligations. This resource diversion weakens the overall cyber resilience of the EU.

- To address this, we recommend the creation of a **single, unified reporting regime,** whereby businesses report incidents according to a one-stop-shop principle to a single point of entry, preferably in the country of main establishment. To ensure a holistic approach and improve the reporting framework this should apply for all entities that are in scope of several legal acts (e.g. NIS2 and CRA). For example, incidents under CRA, NIS2 and sector specific legislation should be reported to national CSIRTs, which shall inform sectoral regulators where appropriate. This would allow businesses to fulfil their regulatory obligations primarily through one national authority in the EU, which will pass on the required information to ENISA and other responsible EU-level authorities, thereby streamlining reporting and enforcement.

- There should be a **harmonised process** that allows companies to report all the information that is required of them as well as track the reports they have provided. This centralisation would ensure greater efficiency, reduce administrative burdens, and improve data quality for incident trend analysis. In addition, **incident notification requirements should be risk-based and proportionate**, with clearer definitions of incident severity thresholds, which are based on impact on confidentiality, integrity or service availability.

- Both NIS2 and CRA are missing **liability clauses** which are necessary for allowing the information to be shared in a more controlled manner. While Art 23(1) of NIS2 points that notification shall not subject the notifying entity to increased liability, the law should also clarify that they should not be liable for potential spill-over effects caused by the act of notification.

- Before a regulator can penalise for non-compliance or failure to report an incident, there should be a **grace period** after regulator notification, to comply with law by submitting a compliant incident report

Supply chain security

The EU cybersecurity regulatory framework needs to address supply chain security more comprehensively. We propose amending the existing regulations to strengthen the security of ICT supply chains, beyond the measures originally proposed within the Cybersecurity Act:

- **Adopting a risk-based classification of the digital supply chain** (including ICT components and service providers) similar to the proportionality approach outlined in DORA, to help prioritise oversight and controls where risk is highest. We also encourage the integration of proposals from our "Common risk-based approach for the Digital Supply Chain" publication, particularly regarding the use of clear baseline cybersecurity fundamentals suppliers must address, the risk-based assessment of criticalities in the digital supply chain and the verification process.

Conclusion

The Charter of Trust is committed to collaborating with the European Commission and other stakeholders to enhance the cybersecurity landscape in Europe. We believe that the proposed recommendations will contribute to a more resilient and secure digital ecosystem. We look forward to continued engagement and providing further input as the revision process progresses.

About the Charter of Trust

The Charter of Trust (EU Transparency Register: 399826651343-07) is a non-profit alliance of leading global companies and organisations working across sectors to make the digital world of tomorrow a safer place. It was founded in 2018 at the Munich Security Conference to enhance cybersecurity efforts and foster digital trust in the face of an increasingly complex and severe cyber threat landscape.

Allianz Atos BOSCH Danfoss elastic IBM
Infineon Microsoft MITSUBISHI HEAVY INDUSTRIES SIEMENS TÜV Founding Partner msc

A unique initiative underpinned by 10 principles fundamental to a secure digital world, the Charter of Trust is working to protect our increasingly digitized world and build a reliable foundation on which trust and digital innovation can flourish. It contributes to the development of effective cybersecurity policies that strengthen global cybersecurity posture and provides expertise on topics including AI, security by default, supply chain security, and education.