European Cyber Security Organisation (ECSO) – Contribution to the European Commission's public consultation on the Cyber Resilience Act

Executive summary

ECSO's members believe that the Cyber Resilience Act (CRA) should constitute the cornerstone of all the cybersecurity regulation in the European Union by providing **horizontal principles** and promoting **consistency and harmonisation** with existing, forthcoming, and revised sectoral legislation

The CRA should have a **broad scope** and include all digital services and devices that could represent a security risk. **Standalone software should be kept out of the scope of the CRA** as it has very specific applications (dominated by the implementation environment and context of use).

Risk categorisation should be identified according to the destination of a product and the risk environment in which it will operate, not just its technical characteristics.

The CRA should require **security by design and by default** to strengthen the resiliency of all digital products and ancillary services, mandate implementation of minimum-security requirements and other best practices like **security updates throughout the products life cycle**, encryption for data at rest and data in transfer as well as Multi-Factor Authentication (MFA) for all products addressed to the consumer market.

ECSO believes that the producers of digital products, across the entire supply chain, should be required to design their products following the principles of SecDevOps and Zero Trust.

The CRA should encourage the creation and implementation of an **EU-wide Vulnerability Disclosure Policy** (VDP) together with bug bounty programmes to reward cybersecurity researchers for their work and ensure a safer online environment.

ECSO encourages the creation of an **EU-wide cybersecurity label** to transparently inform businesses and end-consumers, that are not IT experts, on the origins of each product, its cybersecurity level, and its environmental impact. This label should be very simple to read and would not replace existing certification schemes, but it could be used to encourage the consumption of digital devices and services produced in the EU that comply with EU legislation and standards. ECSO believes that trustworthy EU solutions, meeting stringent security standards, can gain a unique selling point that can differentiate them from cheaper unsecure solutions.

1. Scope

The European Cyber Security Organisation (ECSO), representing the backbone of the European cyber ecosystem, welcomes an ambitious proposal on the upcoming Cyber Resilience Act. In this crucial moment when cyberattacks from state and non-state actors threaten private and public IT systems, ECSO members actively contribute and support **European strategic autonomy, Digital Sovereignty**, and **Cyber Resilience**.

The CRA should not restrict itself to consumer products, services, and processes, but should also include business-to-business (B2B) goods and services, as well as public services. Unlike the NIS Directive and sectoral legislation, the CRA would extend to non-critical sectors and establish a "baseline" which various instances of *lex specialis* could build on. The CRA should therefore be seen as **the minimum baseline for products and services across all sectors**, and thus as the "default regime" to which sectorial legislation can add additional requirements if needed.

The scope of the CRA should extend beyond radio-connected devices to cover all digital devices, as well as digital services and processes. ECSO supports the European Commission's efforts to take a **horizontal approach** to enhancing the cybersecurity of ICT products and services, promoting greater cross-ecosystem consistency in the EU's single market.

ECSO believes that **trustworthy EU solutions, meeting stringent security standards can gain a unique selling point** that can differentiate them from cheaper unsecure solutions.

European Cyber Security Organisation (ECSO) • https://www.ecs-org.eu
EU Transparency registry: 684434822646-91 Rue Ducale, 29, 1000 Brussels Belgium

ECSO encourages the adoption of robust cybersecurity requirements for all digital services and devices that could represent a security risk. In this sense, **standalone software should be left out of the scope of the CRA** as it is mainly adopted for very specific solutions. Avoiding overlapping and potentially contradictory requirements is essential, and established policy frameworks addressing specific sectors should be considered when addressing any new relevant security requirements in standalone software. At EU-level, examples of instruments that have security requirement implication for stand-alone software used in critical sectors include, RED, Cybersecurity Act, GDPR and NIS2. EU Member States implementation of NIS1, European Electronic Communications act, including technical measures stipulated by the 5G toolbox have also introduced additional security requirements. To this end, particular care would be required to ensure that overlaps and potential contradictions are avoided with instruments/requirements at EU as well as national level.

Consistency and harmonisation with existing, forthcoming, and revised sectoral legislation is considered by ECSO the best way forward to help the private sector comply with EU law. ECSO believes that the CRA should simplify and streamline the requirements and certification schemes to help private companies – especially SMEs – and organisations comply with the legislation.

2. Key measures

2.1 Risk categorisation and conformity assessment

The CRA should require suppliers and producers to **provide minimum cybersecurity standards** and encourage them to apply higher ones. This approach is consistent with product regulation under the New Legislative Framework (NLF) and considers the need for compliance before and after products are placed on the market or put into service.

Risk categorisation should be identified according to the destination of a product and the risk environment in which it will operate, not just its technical characteristics.

The digital product or service under the scope of the CRA should pass a **conformity assessment** both first party and third-party (from a Conformity Assessment Body). Conformity assessment can only increase cybersecurity if it is supported by effective market surveillance. Reducing the number of unlawful market participants who create competitive advantages for themselves through insufficient compliance efforts is critical to achieving the targets. Sanctions against non-compliant market participants must be severe and thus have a deterrent effect.

The products under the scope of the CRA should bear a statement that is easily readable and understandable to businesses and end-user so that they can make an informed choice while acquiring secure products and services, even if they are not experts in IT**. An informative EU-wide cybersecurity label should be adopted, indicating origin of the product, cybersecurity level, and environmental impact** of each digital product. This label would not replace existing certification schemes, it would simply inform businesses and end-users and help them to compare similar products.

2.2 Security requirements

Consistency across both basic and elevated requirements is important, as is adjusting approaches to conformity assessment according to scope, goals, and operating environment. The scope and requirements should be future-proof and able to include **emerging technologies** by **focusing on the desired outcomes** rather than prescribing specific implementations. This approach enables the industry to evolve and innovate while still addressing the risks and minimizing requirement obsolescence over time.

The baseline cybersecurity requirements to be introduced by the CRA should apply to all manufacturers and suppliers of tangible and intangible digital products and ancillary services. Both hardware and software – which may be present within the device natively or through additional non-embedded software, as well as on backend services – should be designed, produced, configured, maintained, and decommissioned with **privacy**

and security in mind by design and by default to strengthen resilience.

ECSO believes that the producers of digital products, across the entire supply chain, should be required to design their products following the principles of **SecDevOps** and **Zero Trust**. Producers should also be required to adopt encryption for data at rest and data in transfer for all products addressed to the consumer market as well as Multi-Factor Authentication (MFA).

ECSO believes that a **Vulnerability Disclosure Policy** (VDP), as part of a security by design approach, should become the cornerstone principle and a standard of the European market. Developing a European standard for VDP will contribute to boosting the EU's leadership on the global market.

ECSO strongly supports the idea that all the producers and suppliers of digital services and products in the scope of the CRA should adopt a Vulnerability Disclosure Policy (VDP) as horizontal cybersecurity requirement for all digital products and ancillary services that are placed on the European market. This approach should cover the **whole life cycle of the product**. Adopting a vulnerability disclosure policy facilitates the emergence of collective cybersecurity responsibility which will increase the trust in the digital market. The European Union through the CRA proposal should implement a harmonised approach to mandate the use of VDP and should incentive supply- side actors in treating vulnerabilities more effectively, by providing economic and legal incentives to the adoption of VDP solutions implementing global standards.

In addition to VDP practices, over the last ten years, public authorities, SME, and large corporate have even launched **bug bounty programs** leveraging the collective knowledge and skillsets of the crowd to hunt for technical vulnerabilities and business logic errors alike. Ethical hackers thus make significant contributions to increasing digital security. Furthermore, Bug Bounty is an agile and easy-to-scale security testing model that fits organisations of all sizes and budget breadth and throughout the entire products life cycle**.**

The CRA should also promote innovative methods, such as the Supply Chain Integrity Model (SCIM), that strives to address issues with resources and risk assessment while also offering new capabilities as the **trusted sharing of threat intelligence data.**

Finally, the CRA should promote investments to enhance the cybersecurity of ICT products and services both today and in the future, by pushing the **re-skilling and up-skilling of the workforce** to meet the need of the market.

About ECSO

The European Cyber Security Organisation (ECSO) is a non-for-profit organisation, established in 2016 to support the Public – Private Partnership on cybersecurity with the European Commission. ECSO unites more than 270 European cybersecurity stakeholders, including large companies, SMEs and start-ups, research centres, universities, end-users, operators, associations, and national administrations. ECSO works with its Members and Partners to develop a competitive European cybersecurity ecosystem providing trusted cybersecurity solutions and advancing Europe's cybersecurity posture and its technological independence.

More information: www.ecs-org.eu .

Contact person

For any questions or comment feel free to contact Francesco BORDONE – Junior Manager for Cybersecurity Policies, Legislation, and Market at ECSO. Email francesco.bordone@ecs-org.eu T: +32 492 11 36 72

European Cyber Security Organisation (ECSO)

ECSO is registered at the EU Transparency registry: 684434822646-91