Funded by the European Union

Cyber Resilience Act

Policy brief

Weblink	http://data.europa.eu/eli/reg/2024/2847/oj
Relevance	☐ National policy ☐ EU policy X other: Regulation (EU)
Briefing done by	Peppy Florou

Short summary of the policy

The **Cyber Resilience Act (2024/2847)** is a regulation designed to improve the cybersecurity of products with digital elements throughout their lifecycle. It mandates that manufacturers integrate cybersecurity measures during the design phase and ensure ongoing security through regular updates and vulnerability management. The regulation applies to a wide range of products, including both hardware and software, and sets clear requirements for vulnerability disclosure, risk assessment, and product monitoring. Manufacturers must also ensure secure disposal of products. Market surveillance measures are introduced to ensure compliance, and penalties are set for non-compliance (notably, fines or restrictions on market access for non-compliant products).

By establishing these standards, the Act aims to protect users from cybersecurity threats, reduce vulnerabilities in digital products, and increase trust in the digital ecosystem across the EU. Additionally, it addresses the issue of "security by design," ensuring that cybersecurity is an integral part of product development. The Act also requires manufacturers to implement effective risk management processes and take necessary actions to reduce potential cybersecurity risks associated with their products. For example, a manufacturer of IoT devices will need to integrate automatic security updates and a system for reporting vulnerabilities.

This regulation enhances the EU's overall cyber resilience by ensuring that digital products and services are secure and that risks are managed proactively. Through its comprehensive approach, the Cyber Resilience Act aligns with broader EU cybersecurity efforts, aiming to safeguard the European digital single market against increasing cyber threats.

By focusing on securing the entire lifecycle of digital products and enhancing the response to emerging vulnerabilities, the Cyber Resilience Act represents a significant step forward in establishing a robust and secure digital environment. It is particularly focused on protecting critical sectors and consumers, ensuring that cybersecurity is maintained at every stage of product use, from deployment to decommissioning.

Main objectives of the policy (in bullet points)

The main objectives of the **Cyber Resilience Act** (CRA) are:

- **Enhance cybersecurity** for products with digital elements throughout their lifecycle.
- **Ensure secure design** and development of products, integrating cybersecurity from the start.
- **Regular updates and vulnerability management** to address emerging threats.
- **Mandatory disclosure of security vulnerabilities** to users and authorities.
- **Improve market surveillance** to ensure compliance and address non-compliant products.
- **Strengthen EU resilience** by protecting users and sectors from cybersecurity risks.
- **Increased awareness** of the cybersecurity of digital products for end users and businesses.

Context and relation to DIGITAL EUROPE

The **Cyber Resilience Act** aligns closely with the **Digital Europe Programme (DEP)**, which focuses on bolstering Europe's digital capabilities and infrastructure. DEP aims to advance areas such as cybersecurity, high-performance computing, and artificial intelligence, all of which benefit from the CRA's focus on secure digital product design. Specifically, the CRA:

- **Supports DEP's Cybersecurity Objectives**: By mandating security-by-design principles, the CRA reinforces DEP's goal of enhancing EU-wide cybersecurity infrastructure and resilience.
- **Facilitates Market Development**: The CRA's harmonized rules complement DEP's investment in building a competitive digital single market, ensuring safer products and boosting consumer trust.
- **Addresses Skills Gaps**: DEP's initiatives to develop a skilled digital workforce are essential for implementing CRA's provisions, as the Act depends on professional expertise to achieve compliance.
- **Enhances Strategic Autonomy**: Both initiatives aim to reduce Europe's reliance on external suppliers by fostering local innovation and leadership in secure digital technologies.

By integrating with the DEP, the CRA strengthens the EU's vision for a resilient, inclusive, and competitive digital ecosystem, essential for achieving the objectives of Europe's Digital Decade.

What parts of the Policy are directly related to specific objectives (SO) in DEP

The **Cyber Resilience Act** aligns with several **Specific Objectives (SOs)** of **DEP** by addressing key areas of cybersecurity, digital trust, and technology resilience:

SO1: High Performance Computing (HPC)

- **Link**: CRA's security standards can benefit from HPC technologies in the development and testing of secure digital products, enabling better performance in threat analysis and mitigation.
- **Reason for proposers**: Projects involving HPC for cybersecurity can help meet CRA compliance, aligning with DEP's support for high-performance computing solutions.

SO2: Artificial Intelligence (AI)

- **Link**: The CRA encourages the use of AI for enhancing product security and vulnerability detection.
- **Reason for proposers**: AI-driven cybersecurity solutions can assist in meeting CRA's secure-by-design requirements, benefiting DEP's AI focus.

SO3: Cybersecurity and Trust

- **Link**: The CRA directly supports this objective by setting cybersecurity requirements for digital products, ensuring their trustworthiness across sectors.
- **Reason for proposers**: Proposals that strengthen cybersecurity solutions are key to aligning with CRA mandates and DEP goals in trust-building and EU-wide security.

SO4: Advanced Digital Skills

- **Link**: The CRA emphasizes the need for a skilled workforce to ensure compliance with cybersecurity standards.
- **Reason for proposers**: Proposals focused on cybersecurity training and certification will align with both DEP and CRA objectives, addressing the growing skill gap.

SO5: Deployment and Best Use of Digital Capacities and Interoperability

- **Link**: The CRA promotes secure, interoperable products that align with EU standards for digital infrastructure.
- **Reason for proposers**: Proposals developing secure, interoperable solutions will support both the CRA and DEP objectives of enhancing digital infrastructure.

Which activities in the current DEP Work Programme contribute to meeting the objectives of the policy

DEP has launched several calls for proposals that align with the objectives of the **Cyber Resilience Act**, focusing on enhancing cybersecurity, digital trust, and technological resilience across the European Union. Below is a detailed list of these calls, their objectives, and how they contribute to meeting the CRA's goals:

National SOCs
Call ID: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOC
Objective: To establish or strengthen National Security Operations Centers (SOCs) equipped with advanced tools for monitoring, understanding, and proactively managing cyber events. These centers will collaborate closely with relevant entities such as Computer Security Incident Response Teams (CSIRTs) and utilize aggregated data to provide early warnings to critical infrastructures.
Contribution to CRA: Enhances national cybersecurity capabilities, ensuring that digital products and services meet robust security standards throughout their lifecycle.

Enlarging existing or Launching New Cross-Border SOC Platforms
Call ID: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOCPLAT
Objective: To strengthen cross-border SOC platforms by facilitating data sharing and joint development of cyber detection, analysis, and prevention capabilities in a trusted environment.
Contribution to CRA: Promotes interoperability and data exchange between SOC platforms, aligning with the CRA's emphasis on secure digital product design and lifecycle management.

Strengthening the SOC Ecosystem
Call ID: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOCSYS
Objective: To empower SOCs linked to National SOCs, fostering collaboration between local, national, and cross-border SOCs. This initiative aims to enhance data sharing and detection capabilities for cyber threats.
Contribution to CRA: Supports the CRA's objective of ensuring that interconnected products meet robust cybersecurity criteria, thereby strengthening the digital supply chain.

Development and Deployment of Advanced Key Technologies
Call ID: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-KEYTECH
Objective: To enable European cybersecurity actors to leverage breakthroughs in key digital technologies such as Artificial Intelligence (AI), Big Data Analytics, Quantum Computing, Blockchain Technology, High-Performance Computing, and Software-Defined Networking. These technologies aim to improve detection and prevention capabilities, efficiency, scalability, and facilitate data sharing and regulatory compliance.

Contribution to CRA: Aligns with the CRA's focus on integrating advanced technologies to enhance the security and resilience of digital products and services.

Preparedness Support and Mutual Assistance, Targeting Larger Industrial Operations and Installations
Call ID: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER
Objective: To complement efforts by Member States and the Union in increasing protection and resilience against cyber threats for large industrial installations and infrastructures. This includes providing knowledge and expertise to improve preparedness for cyber threats and incidents.
Contribution to CRA: Ensures that critical infrastructures adhere to high cybersecurity standards, supporting the CRA's objective of secure-by-design principles.

Support for Implementation of EU Legislation on Cybersecurity and National Cybersecurity Strategies (2024)
Call ID: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-CYBERSEC-02
Objective: To support the implementation of EU cybersecurity legislation, including the NIS2 Directive and the Cybersecurity Act, and to enhance cooperation at technical, operational, and strategic levels. This action also aims to support the implementation of the proposed Cyber Resilience Act by increasing the capacities of market surveillance authorities, notifying authorities, and national accreditation bodies.
Contribution to CRA: Directly supports the CRA's implementation, ensuring effective enforcement and compliance across Member States.

These calls are open for submissions from 4 July 2024, until 27 March 2025.

By participating in these calls, proposers can contribute to the EU's cybersecurity objectives, align with the CRA's requirements, and enhance the security and resilience of digital products and services across Europe.

Please match any specific activity mentioned in the policy with concrete call topics from the current/upcoming DEP Work Programme

See above

Events

For finding related events, please check out the following online calenders: Shaping Europe's digital future, ECCC