CYBERSECURITY SOLIDARITY ACT

Policy briefing

Weblink	http://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity
Relevance	☐ National policy x EU policy ☐ other: ____________________
Briefing done by	Mélina Di Matteo, UWE

Short summary of the policy

Adopted by the European Commission in April 2023, the Cybersecurity Solidarity Act entered into force on 4 February 2025. The Act strengthens the EU's collective ability to detect, prepare for, and respond to large-scale cyberattacks. Aimed at closing the gaps in cooperation and responsiveness to cross-border cyber threats – including those targeting critical infrastructure – it comes against a backdrop of growing geopolitical tensions and hybrid threats.

The text proposes a strengthening of the European cybersecurity framework through the creation of new operational structures and instruments, in particular:

- The **Cybersecurity Emergency Mechanism** to improve preparedness, support mutual assistance, and enable the deployment of capacities such as Cyber Rapid Response Teams.
- Support for the deployment of **interconnected SOCs**, forming the European Cyber Shield.
- A **cybersecurity reserve** of pre-qualified service providers, rapidly mobilized to support Member States in the event of major cyber incidents.

The Act also aims to improve resilience through coordinated penetration testing, joint response exercises, and enhanced information sharing between national authorities, European institutions, and the private sector.

Main objectives of the policy

- Detect cyberthreats rapidly through an EU-wide network of SOCs.
- Enable a coordinated and collective response to major cross-border cybersecurity incidents.
- Strengthen solidarity between Member States through coordinated response mechanisms.
- Improve preparedness for cyber crises (exercises, assessments, joint responses).
- Create a pool of cybersecurity services that can be mobilized in the event of an incident.
- Increase operational cooperation between Member States, ENISA, and the Commission.

The DEP4ALL project is funded by the European Commission under the Digital Europe Programme, under grant agreement no. 101167919. Any opinions expressed in these pages are those of the author/organisation and do not necessarily reflect the views of the European Commission.

Context and relation to the Digital Europe Programme (DEP)

In general, DEP supports the implementation of the Cybersecurity Solidarity Act by funding actions that improve detection, preparedness, and coordinated responses to large-scale cyber incidents across the EU:

CYBERSECURITY SOLIDARITY ACT	DEP
European Cyber Shield	Funds the deployment and interconnection of SOCs to enable real-time threat detection and rapid coordinated responses.
Cybersecurity Emergency Mechanism	Supports preparedness actions, mutual assistance mechanisms, and the establishment of Cyber Rapid Response Teams through dedicated funding for cross-border cyber crisis response.
Cybersecurity Reserve	Finances the setup and maintenance of a pool of trusted service providers ready to assist during major cyber incidents across Member States.
Collective cyber crisis management	Supports initiatives that improve coordination between Member States, the Commission, ENISA, and other stakeholders for effective EU-wide incident response.
Testing and exercises	Funds penetration testing, simulated crisis response exercises, and vulnerability assessments across critical sectors.
Operational cooperation and solidarity	Promotes joint actions, common tools, and harmonised procedures to enhance interoperability and mutual support in case of cyber emergencies.
Implementation of EU legislation	Provides financial and technical assistance to help Member States and operators meet their legal obligations under the new cybersecurity regulatory framework.

Parts of the policy directly related to Specific Objectives (SO) in DEP

SO1 – HPC: While not explicitly addressed in the Act, it aligns with the emphasis on coordinated preparedness and adoption of cutting-edge technologies for resilience.

SO2 – AI Continent: Several calls use AI to enhance cyber resilience.

SO3 – Cybersecurity: The Cybersecurity Solidarity Act is most directly linked to SO3. It introduces concrete mechanisms (European Cyber Shield, Cybersecurity Emergency Mechanism, and Cybersecurity Reserve), which align with multiple DEP calls.

SO4 – Advanced Digital Skills: Support the training of cybersecurity professionals, in line with the Act's focus on operational readiness.

SO5 – Accelerating the best use of Digital Capacities: Align with the Act's emphasis on coordinated preparedness and adoption of cutting-edge technologies for resilience.

SO6 – Semiconductors: Not a primary focus of the Cybersecurity Solidarity Act, but semiconductor security and supply chain resilience are implicit enablers of the Act's objectives.

The DEP4ALL project is funded by the European Commission under the Digital Europe Programme, under grant agreement no. 101167919. Any opinions expressed in these pages are those of the author/organisation and do not necessarily reflect the views of the European Commission.

Activities in the DEP Work Programme 2025-27 contributing to the objectives of the policy

1. Building the European Cybersecurity alert system through National and Cross-Border Cyber Hubs

The Cyber Solidarity Act aims to establish a European Cybersecurity Alert System based on a network of National and Cross-Border Cyber Hubs. These hubs strengthen early threat detection, analysis, and real-time information sharing across the EU.

Relevant DEP 2026–27 calls:

- **National Cyber Hubs** (Call for Expression of Interest, simple grant, EUR X million): select contracting authorities that will participate in a joint procurement for the creation or reinforcement of National Cyber Hubs, as part of the establishment of the European Cybersecurity Alert System.
- **Enhancing the NCC Network** (simple grant, EUR 46 million): supports the development and interconnection of National Cybersecurity Coordination Centre.
- **Cross-Border Cyber Hubs** (Call for Expression of Interest, EUR 30 million): promotes transnational collaboration and interoperability between Member States.

These topics operationalise the Act's objective of creating a shared detection infrastructure and improved situational awareness at European level.

2. Strengthening the Cyber Hubs Ecosystem and Enhancing Information Sharing

To ensure interoperability and efficiency, the Act calls for harmonised tools, shared data standards, and collective training.
Relevant DEP topic: Strengthening the Cyber Hubs Ecosystem and Enhancing Information Sharing (CSA, EUR 2 million)

Policy link: This topic supports the development of common procedures and data-exchange standards between hubs, as well as training and joint exercises aligned with the European Cybersecurity Skills Framework.

3. Enhancing Collective Preparedness and Coordinated Response

Another component of the Cyber Solidarity Act is the ability to jointly test and improve Europe's cyber crisis response through coordinated preparedness exercises.
Relevant DEP topics: Coordinated Preparedness Testing and Other Preparedness Actions (2026–2027 – Simple Grants, EUR 5 / 15 / 20 million)

Policy link: These actions fund large-scale cross-border and cross-sector preparedness exercises, improving EU-level readiness and aligning crisis management procedures.

4. Mutual Assistance and European Solidarity During Major Incidents

The Act introduces a mutual assistance mechanism enabling technical and operational support between Member States during significant cyber incidents.
Relevant DEP topic: Mutual Assistance (2026–2027 – Grants for Named Beneficiaries, EUR 2 million per year)
Policy link: These actions make the solidarity mechanism operational, ensuring rapid deployment of expert support teams and shared EU-level response capacity.

The DEP4ALL project is funded by the European Commission under the Digital Europe Programme, under grant agreement no. 101167919. Any opinions expressed in these pages are those of the author/organisation and do not necessarily reflect the views of the European Commission.

Related policies and further information

General information on the EU cybersecurity policies: *EU cybersecurity policies*

Related *policies:*

- Directive (EU) 2022/2555 – NIS 2 Directive
- EU Cybersecurity Act
- Cyber Resilience Act
- EU Cybersecurity Strategy for the Digital Decade

For related events, please check out the online calendar: Shaping Europe's digital future

The DEP4ALL project is funded by the European Commission under the Digital Europe Programme, under grant agreement no. 101167919. Any opinions expressed in these pages are those of the author/organisation and do not necessarily reflect the views of the European Commission.