EU Cyber Solidarity Act –

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents

EU Cyber Solidarity Act

Proposed in 18 Apr 2023

Broad Goal: Strengthen capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents through the following actions:

- Deployment of a pan-European infrastructure of Security Operations Centres (‘European Cyber Shield’) to build and enhance common detection and situational awareness capabilities;
- Creation of a Cybersecurity Emergency Mechanism to support Member States in preparing for, responding to, and immediate recovery from significant and largescale cybersecurity incidents
- Establish a European Cybersecurity Incident Review Mechanism to review and assess significant or large-scale incidents

EU Cyber Solidarity Act

Objectives:

- Strengthen common Union detection and situational awareness of cyber threats and incidents thus allowing to reinforce the competitive position of industry and services sectors in the Union across the digital economy and contribute to the Union's technological sovereignty in the area of cybersecurity;
- Reinforce preparedness of entities operating in critical and highly critical sectors across the Union and strengthen solidarity by developing common response capacities against significant or large-scale cybersecurity incidents, including by making Union cybersecurity incident response support available for third countries associated to the Digital Europe Programme ('DEP');
- Enhance Union resilience and contribute to effective response by reviewing and assessing significant or large-scale incidents, including drawing lessons learned and, where appropriate, recommendations

EU Cyber Solidarity Act
Key Definitions

- **Cross-border Security Operations Centre ("Cross-border SOC"):** A multi-country platform that brings together in a coordinated network structure national SOCs from at least three Member States who form a Hosting Consortium, and that is designed to prevent cyber threats and incidents and to support the production of high-quality intelligence, notably through the exchange of data from various sources, public and private, as well as through the sharing of state-of-the-art tools and jointly developing cyber detection, analysis, and prevention and protection capabilities in a trusted environment
- **public body:** A body governed by public law as defined in Directive 2014/24/EU of the European Parliament and the Council
- **entity:** An entity as defined in Directive (EU) 2022/2555
- **trusted providers:** Managed security service providers as defined in of Directive (EU) 2022/2555 selected in accordance with this Regulation

EU Cyber Solidarity Act
European Cyber Shield

Establish an interconnected pan-European infrastructure of Security Operations Centres ('European Cyber Shield') to develop advanced capabilities for the Union to detect, analyse and process data on cyber threats and incidents in the Union

European Cyber Shield is to :

- Pool and share data on cyber threats and incidents from various sources through cross-border SOCs;
- Produce high-quality, actionable information and cyber threat intelligence, through the use of state-of-the art tools, notably Artificial Intelligence and data analytics technologies;
- Contribute to better protection and response to cyber threats;
- Contribute to faster detection of cyber threats and situational awareness across the Union;
- Provide services and activities for the cybersecurity community in the Union, including contributing to the development advanced artificial intelligence and data analytics tools.

EU Cyber Solidarity Act
National Security Operations Centres

To participate in the European Cyber Shield, each Member State is to designate at least one National Security Operations Centre (SOC). The National SOC is to be a public body

The National SOC is to:

- Have the capacity to act as a reference point and gateway to other public and private organisations at national level for collecting and analysing information on cybersecurity threats and incidents and contributing to a Cross-border SOC
- Be equipped with state-of-the-art technologies capable of detecting, aggregating, and analysing data relevant to cybersecurity threats and incidents
- Be selected by the European Cybersecurity Competence Centre (‘ECCC’) to participate in a joint procurement of tools and infrastructures with the ECCC
- Commit to apply to participate in a Cross-border SOC within two years from the date on which the tools and infrastructures are acquired, or on which it receives grant funding, whichever occurs sooner

EU Cyber Solidarity Act
Cross-Border Security Operations Centres

- Hosting Consortium consisting of at least three Member States, represented by National SOCs, committed to working together to coordinate their cyber-detection and threat monitoring activities are to be eligible to participate in actions to establish a Cross-border SOC
- Hosting Consortium is to be selected by the ECCC to participate in a joint procurement of tools and infrastructures with the ECCC. Before launching the procedure for the acquisition of the tools and infrastructures, the ECCC and the Hosting Consortium is to conclude a hosting and usage agreement regulating the usage of the tools and infrastructures
- Members of the Hosting Consortium are to conclude a written consortium agreement which sets out their internal arrangements for implementing the hosting and usage Agreement
- A Cross-border SOC is to be represented for legal purposes by a National SOC acting as coordinating SOC, or by the Hosing Consortium if it has legal personality
- The co-ordinating SOC is to be responsible for compliance with the requirements of the hosting and usage agreement and of this Regulation

EU Cyber Solidarity Act
Cross-Border Security Operations Centres

- Members of a Hosting Consortium are to exchange relevant information among themselves within the Cross-border SOC including information relating to cyber threats, near misses, vulnerabilities, techniques and procedures, indicators of compromise, adversarial tactics, threat-actor-specific information, cybersecurity alerts and recommendations regarding the configuration of cybersecurity tools to detect cyber attacks, where such information sharing:
  - Aims to prevent, detect, respond to or recover from incidents or to mitigate their impact;
  - Enhances the level of cybersecurity, in particular through raising awareness in relation to cyber threats, limiting or impeding the ability of such threats to spread, supporting a range of defensive capabilities, vulnerability remediation and disclosure, threat detection, containment and prevention techniques, mitigation strategies, or response and recovery stages or promoting collaborative threat research between public and private entities
  - Supports the development of an EU Cyber Shield, including the development, deployment and operation of National and Cross-border SOCs platforms that contribute to situational awareness in the Union and to enhancing the cyber threat intelligence capacities of the Union
  - Establishes and operates a Cyber Emergency Mechanism to support Member States in preparing for and responding to significant cybersecurity incidents, complementary to national resources and capabilities and other forms of support available at Union level, including the establishment of an EU Cybersecurity Reserve
- 2. The actions under Specific Objective 3 is to be implemented primarily through the European Cybersecurity Industrial, technology and research Competence Centre and the Network of National Coordination Centres, in accordance with Regulation (EU) 2021/887 of the European Parliament and of the Council with the exception of actions implementing the EU Cybersecurity Reserve, which are to be implemented by the Commission and ENISA

EU Cyber Solidarity Act
Cross-Border Security Operations Centres

- To encourage exchange of information between Cross-border SOCs, Cross-border SOCs are to ensure a high level of interoperability between themselves
- To facilitate the interoperability between the Cross-border SOCs, the Commission may, by means of implementing acts, after consulting the ECCC, specify the conditions for this interoperability
- Cross-border SOCs are to conclude cooperation agreements with one another, specifying information sharing principles among the cross-border platforms
- Where the Cross-border SOCs obtain information relating to a potential or ongoing largescale cybersecurity incident, they are to provide relevant information to EU-CyCLONe, the CSIRTs network and the Commission, in view of their respective crisis management roles without undue delay
- The Commission may, by means of implementing acts, determine the procedural arrangements for the information sharing

EU Cyber Solidarity Act Security Concerns

Member States participating in the European Cyber Shield are to:

- Ensure a high level of data security and physical security of the European Cyber Shield infrastructure
- Ensure that the infrastructure is adequately managed and controlled in such a way as to protect it from threats
- Ensure its security and that of the systems, including that of data exchanged through the infrastructure.
- Ensure that the sharing of information within the European Cyber Shield with entities which are not Member State public bodies does not negatively affect the security interests of the Union.

The Commission may adopt implementing acts laying down technical requirements for Member States to comply with their obligation under this Regulation. Those implementing acts are to be adopted in accordance with the examination procedure per this Regulation. The Commission is to take into account relevant defence-level security standards, in order to facilitate cooperation with military actors

EU Cyber Solidarity Act
Cyber Emergency Mechanism

Establish a Cyber Emergency Mechanism to improve the Union's resilience to major cybersecurity threats and prepare for and mitigate the short-term impact of significant and large-scale cybersecurity incidents (the 'Mechanism')

The Mechanism is to support the following types of actions:

- Preparedness actions, including the coordinated preparedness testing of entities operating in highly critical sectors across the Union;
- Response actions, supporting response to and immediate recovery from significant and large-scale cybersecurity incidents, to be provided by trusted providers participating in the EU Cybersecurity Reserve;
- Mutual assistance actions consisting of the provision of assistance from national authorities of one Member State to another Member State

EU Cyber Solidarity Act
EU Cybersecurity Reserve

Establish a EU Cybersecurity Reserve to assist in responding or providing support for responding to significant or large-scale cybersecurity incidents, and immediate recovery from such incidents

- Consists of incident response services from trusted providers selected in accordance with the criteria laid down in this Regulation
- Include pre-committed services deployable in all Member States.
- Users of the services from the EU Cybersecurity Reserve are to include:
  - Member States' cyber crisis management authorities and CSIRTs
  - Union institutions, bodies and agencies
- Users use the services from the EU Cybersecurity Reserve to respond or support response to and immediate recovery from significant or large-scale incidents affecting entities operating in critical or highly critical sectors
- The Commission has overall responsibility for the implementation of the EU Cybersecurity Reserve, determines the priorities and evolution of the EU Cybersecurity Reserve, supervises its implementation, and ensure complementarity, consistency, synergies and links with other support actions under this Regulation as well as other Union actions and programmes

EU Cyber Solidarity Act
EU Cybersecurity Reserve

- The Commission may entrust the operation and administration of the EU Cybersecurity Reserve, in full or in part, to ENISA, by means of contribution agreements.
- To support the Commission in establishing the EU Cybersecurity Reserve, ENISA shall prepare a mapping of the services needed, after consulting Member States and the Commission. ENISA is to prepare a similar mapping, after consulting the Commission, to identify the needs of third countries eligible for support from the EU Cybersecurity Reserve
- The Commission may, by means of implementing acts, specify the types and the number of response services required for the EU Cybersecurity Reserve

EU Cyber Solidarity Act
Request for EU Cybersecurity Reserve Support

- Users may request services from the EU Cybersecurity Reserve to support response to and immediate recovery from significant or large-scale cybersecurity incidents
- To receive support from the EU Cybersecurity Reserve, the users are to take measures to mitigate the effects of the incident for which the support is requested, including the provision of direct technical assistance, and other resources to assist the response to the incident, and immediate recovery efforts
- Requests for support from users referred to in are transmitted to the Commission and ENISA via the Single Point of Contact designated or established by the Member State
- Member States are to inform the CSIRTs network, and where appropriate EU-CyCLONe, about their requests for incident response and immediate recovery support
-

EU Cyber Solidarity Act
Request for EU Cybersecurity Reserve Support

- Requests for incident response and immediate recovery support are to include:
  - Appropriate information regarding the affected entity and potential impacts of the incident and the planned use of the requested support, including an indication of the estimated needs;
  - Information about measures taken to mitigate the incident for which the support is requested, as referred to in paragraph 2;
  - Information about other forms of support available to the affected entity, including contractual arrangements in place for incident response and immediate recovery services, as well as insurance contracts potentially covering such type of incident
- ENISA, in cooperation with the Commission and the NIS Cooperation Group, is to develop a template to facilitate the submission of requests for support from the EU Cybersecurity Reserve
- The Commission may, by means of implementing acts, specify further the detailed arrangements for allocating the EU Cybersecurity Reserve support services

EU Cyber Solidarity Act
Implementation of EU Cybersecurity Reserve Support

- Requests for support from the EU Cybersecurity Reserve is assessed by the Commission, with the support of ENISA or as defined in contribution agreements, and a response is transmitted to the users without delay
- To prioritise requests, in the case of multiple concurrent requests, the following criteria are to be taken into account, where relevant:
  - The severity of the cybersecurity incident;
  - The type of entity affected, with higher priority given to incidents affecting essential entities;
  - The potential impact on the affected Member State(s) or users;
  - The potential cross-border nature of the incident and the risk of spill over to other Member States or users;
  - The measures taken by the user to assist the response, and immediate recovery efforts
- The EU Cybersecurity Reserve services are to be provided in accordance with specific agreements between the service provider and the user to which the support under the EU Cybersecurity Reserve is provided. Those agreements are to include liability conditions

EU Cyber Solidarity Act
Implementation of EU Cybersecurity Reserve Support

- The agreements may be based on templates prepared by ENISA, after consulting Member States
- The Commission and ENISA are to bear no contractual liability for damages caused to third parties by the services provided in the framework of the implementation of the EU Cybersecurity Reserve
- Within one month from the end of the support action, the users are to provide the Commission and ENISA with a summary report about the service provided, results achieved and the lessons learned. When the user is from a third country, such report is to be shared with the High Representative
- The Commission is to report to the NIS Cooperation Group about the use and the results of the support, on a regular basis

EU Cyber Solidarity Act Coordination with Crisis Management Mechanisms

- In cases where significant or large-scale cybersecurity incidents originate from or result in disasters, the support under this Regulation for responding to such incidents is to complement actions under and without prejudice to Decision 1313/2013/EU.
- In the event of a large-scale, cross border cybersecurity incident where Integrated Political Crisis Response arrangements (IPCR) are triggered, the support under this Regulation for responding to such incident is to be handled in accordance with relevant protocols and procedures under the IPCR.
- In consultation with the High Representative, support under the Cyber Emergency Mechanism may complement assistance provided in the context of the Common Foreign and Security Policy and Common Security and Defence Policy, including through the Cyber Rapid Response Teams. It may also complement or contribute to assistance provided by one Member State to another Member State in the context of Article 42(7) of the Treaty on the European Union.
- Support under the Cyber Emergency Mechanism may form part of the joint response between the Union and Member States in situations referred to in Article 222 of the Treaty on the Functioning of the European Union

EU Cyber Solidarity Act
Trusted Providers

- In procurement procedures for the purpose of establishing the EU Cybersecurity Reserve, the contracting authority is to act in accordance with the principles laid down in the Regulation (EU, Euratom) 2018/1046 and in accordance with the following principles:
  - Ensure the EU Cybersecurity Reserve includes services that may be deployed in all Member States, taking into account in particular national requirements for the provision of such services, including certification or accreditation;
  - Ensure the protection of the essential security interests of the Union and its Member States;
  - Ensure that the EU Cybersecurity Reserve brings EU added value, by contributing to the objectives set out in Article 3 of Regulation (EU) 2021/694, including promoting the development of cybersecurity skills in the EU

EU Cyber Solidarity Act
Trusted Providers

- When procuring services for the EU Cybersecurity Reserve, the contracting authority is to include in the procurement documents the following selection criteria:
  - The provider demonstrates that its personnel has the highest degree of professional integrity, independence, responsibility, and the requisite technical competence to perform the activities in their specific field, and ensures the permanence/continuity of expertise as well as the required technical resources;
  - The provider, its subsidiaries and subcontractors have in place a framework to protect sensitive information relating to the service, and in particular evidence, findings and reports, and is compliant with Union security rules on the protection of EU classified information;
  - The provider provides sufficient proof that its governing structure is transparent, not likely to compromise its impartiality and the quality of its services or to cause conflicts of interest;
  - The provider has appropriate security clearance, at least for personnel intended for service deployment;
  - The provider has the relevant level of security for its IT systems;

EU Cyber Solidarity Act
Trusted Providers

- When procuring services for the EU Cybersecurity Reserve, the contracting authority is to include in the procurement documents the following selection criteria:
  - The provider is equipped with the hardware and software technical equipment necessary to support the requested service;
  - The provider is able to demonstrate that it has experience in delivering similar services to relevant national authorities or entities operating in critical or highly critical sectors;
  - The provider is able to provide the service within a short timeframe in the Member State(s) where it can deliver the service;
  - The provider is able to provide the service in the local language of the Member State(s) where it can deliver the service;
  - Once an EU certification scheme for managed security service Regulation (EU) 2019/881 is in place, the provider is to be certified in accordance with that scheme

EU Cyber Solidarity Act
Support to Third Countries

- Third countries may request support from the EU Cybersecurity Reserve where Association Agreements concluded regarding their participation in DEP provide for this.
- Support from the EU Cybersecurity Reserve is in accordance with this Regulation, and complies with any specific conditions laid down in the Association Agreements
- Users from associated third countries eligible to receive services from the EU Cybersecurity Reserve is to include competent authorities such as CSIRTs and cyber crisis management authorities
- Each third country eligible for support from the EU Cybersecurity Reserve is to designate an authority to act as a single point of contact for the purpose of this Regulation
- Prior to receiving any support from the EU Cybersecurity Reserve, third countries are to provide to the Commission and the High Representative information about their cyber resilience and risk management capabilities, including at least information on national measures taken to prepare for significant or large-scale cybersecurity incidents, as well as information on responsible national entities, including CSIRTs or equivalent entities, their capabilities and the resources allocated to them
- The Commission is to coordinate with the High Representative about the requests received and the implementation of the support granted to third countries from the EU Cybersecurity Reserve

EU Cyber Solidarity Act
Cybersecurity Incident Review Mechanism

- At the request of the Commission, the EU-CyCLONe or the CSIRTs network, ENISA is to review and assess threats, vulnerabilities and mitigation actions with respect to a specific significant or large-scale cybersecurity incident. Following the completion of a review and assessment of an incident, ENISA is to deliver an incident review report to the CSIRTs network, the EU-CyCLONe and the Commission to support them in carrying out their tasks. Where relevant, the Commission shall share the report with the High Representative
- To prepare the incident review report referred to above, ENISA is to collaborate all relevant stakeholders, including representatives of Member States, the Commission, other relevant EU institutions, bodies and agencies, managed security services providers and users of cybersecurity services. Where appropriate, ENISA is to also collaborate with entities affected by significant or large-scale cybersecurity incidents. To support the review, ENISA may also consult other types of stakeholders. Consulted representatives shall disclose any potential conflict of interest
- The report is to cover a review and analysis of the specific significant or large-scale cybersecurity incident, including the main causes, vulnerabilities and lessons learned. It is to protect confidential information, in accordance with Union or national law concerning the protection of sensitive or classified information
- Where appropriate, the report is to draw recommendations to improve the Union's cyber posture.
- Where possible, a version of the report is to be made available publicly and only include public information