EUROPEAN
COMMISSION

Strasbourg, 18.4.2023
COM(2023) 209 final

2023/0109 (COD)

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

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

• Reasons for and objectives of the proposal

This explanatory memorandum accompanies the proposal for a Cyber Solidarity Act. The use of and dependence on information and communication technologies have become fundamental aspects in all sectors of economic activity as our public administrations, companies and citizens are more interconnected and interdependent across sectors and borders than ever before. This higher uptake of digital technologies increases exposure to cyber security incidents and their potential impacts. At the same time, Member States are facing growing cybersecurity risks and an overall complex threat landscape, with a clear risk of rapid spill-over of cyber incidents from one Member State to others.

What is more, cyber operations are increasingly integrated in hybrid and warfare strategies, with significant effects on the target. In particular, Russia's military aggression against Ukraine was preceded and is being accompanied by a strategy of hostile cyber operations, which is a game changer for the perception and assessment of the EU's collective cybersecurity crisis management preparedness and a call for urgent action. The threat of a possible large-scale incident causing significant disruption and damage to critical infrastructures demands heightened preparedness at all levels of the EU's cybersecurity ecosystem. That threat goes beyond Russia's military aggression on Ukraine and includes continuous cyber threats from state and non-state actors, which are likely to persist, given the multiplicity of state-aligned, criminal and hacktivist actors involved in current geopolitical tensions. In recent years, the number of cyberattacks has increased dramatically, including supply chain attacks aiming at cyberespionage, ransomware or disruption. In 2020, the SolarWinds supply chain attack affected more than 18,000 organisations globally, including government agencies, major companies. Significant cybersecurity incidents can be too disruptive for a single or several affected Member States to handle alone. For that reason, strengthened solidarity at Union level is required to better detect, prepare and respond to cybersecurity threats and incidents.

As regards detection of cyber threats and incidents, there is an urgent need to increase the exchange of information and improve our collective capacities in order to reduce drastically the time needed to detect cyber threats, before they can cause large-scale damage and costs[1]. While many cybersecurity threats and incidents have a potential cross-border dimension, due to the interconnection of digital infrastructures, the sharing of relevant information among Member States remains limited. Building a network of cross-border Security Operations Centres (SOCs) to enhance detection and response capabilities aims to help address this issue.

As regards preparedness and response to cybersecurity incidents, there is currently limited support at Union level and solidarity between Member States. The Council Conclusions of

[1] According to a report by Ponemon Institute and IBM Security, the average time to identify a breach in 2022 was 207 days, with an additional 70 days to contain. At the same time, in 2022, data breaches with a lifecycle of more than 200 days had an average cost of €4.86 million, compared to €3.74 million when under 200 day. ('Cost of a data breach 2022", https://www.ibm.com/reports/data-breach)

October 2021 highlighted the need to address these gaps, by calling for the Commission to present a proposal on a new Emergency Response Fund for Cybersecurity[2].

This Regulation also implements the EU Cybersecurity Strategy adopted in December 2020[3] that announced the creation of a European Cyber Shield, reinforcing the cyber threat detection and information sharing capabilities in the European Union through a federation of national and cross-border SOCs.

This Regulation builds upon first steps already developed in closed collaboration with the main stakeholders and supported by the Digital Europe Programme (DEP). In particular, on SOCs, a Call for Expression of Interest to jointly procure tools and infrastructure to establish Cross-border SOCs, and a call for grants to enable capacity building of SOCs serving public and private organisations, were held under DEP cybersecurity work programme 2021-2022. As regards preparedness and incident response, the Commission has set up a short-term programme to support Member States, through additional funding allocated to the European Union Agency for Cybersecurity (ENISA), in order to immediately reinforce preparedness and capacities to respond to major cyber incidents. Both actions have been prepared in close coordination with Member States. This Regulation addresses shortcomings and integrates insights from those actions.

Finally, this proposal delivers on the commitment in line with the Joint Cyber Defence Communication[4] adopted on 10 November, to prepare a proposal for an EU Cyber Solidarity Initiative with the following objectives: strengthen common EU detection, situational awareness, and response capabilities, to gradually build an EU-level cybersecurity reserve with services from trusted private providers and to support testing of critical entities.

Against this background, the Commission is putting forward the present Cyber Solidarity Act to strengthen solidarity at Union level in order to better detect, prepare and respond to cybersecurity threats and incidents through the following specific objectives:

- to strengthen common EU detection and situational awareness of cyber threats and incidents, and thus contribute to European technological sovereignty in the area of cybersecurity;
- to reinforce preparedness of critical entities across the EU and strengthen solidarity by developing common response capacities against significant or large-scale cybersecurity incidents, including by making incident response support available for third countries~~.~~ associated to DEP;
- to 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.

---

2 Council conclusions on the development of the European Union's cyber posture approved by the Council at its meeting on 23 May 2022, (9364/22

3 Joint Communication to the European Parliament and the Council, The EU's Cybersecurity Strategy for the Digital Decade, JOIN202018 final.

4 Joint Communication to the European Parliament and the Council, EU Policy on Cyber Defence, JOIN(2022) 49 final.

These objectives shall be implemented through the following actions:

- The deployment of a pan-European infrastructure of SOCs (European Cyber Shield) to build and enhance common detection and situational awareness capabilities.
- The creation of a Cyber Emergency Mechanism to support Member States in preparing for, responding to and immediate recovery from significant and large-scale cybersecurity incidents. Support for incident response shall also be made available to European institutions, bodies, offices and agencies of the Union (EUIBAs).
- The establishment of a European Cybersecurity Incident Review Mechanism to review and assess specific significant or large-scale incidents.

The European Cyber Shield and the Cyber Emergency Mechanism will be supported by funding from the DEP, which this legislative instrument will amend in order to establish the above-mentioned actions, provide for financial support for their development and clarify the conditions for benefitting from the financial support.

- **Consistency with existing policy provisions in the policy area**

The EU framework comprises several legislations already in place or proposed at Union level to reduce vulnerabilities, increase the resilience of critical entities against cybersecurity risks and support the coordinated management of large-scale cybersecurity incidents and crises, notably the Directive on measures for a high common level of security of network and information systems across the Union (NIS2)[5], the Cybersecurity Act[6], the Directive on attacks against information systems[7] the Commission Recommendation (EU) 2017/1584 on coordinated response to large-scale cybersecurity incidents and crises[8].

The actions proposed under the Cyber Solidarity Act cover situational awareness, information sharing, as well as support for preparedness and response to cyber incidents. These actions are consistent with and support the objectives of the regulatory framework in place at Union level, notably under Directive (EU) 2022/2555 ('the NIS2 Directive'). The Cyber Solidarity Act will especially build on and support the existing cybersecurity operational cooperation and crisis management frameworks, in particular European cyber crisis liaison organisation network (EU-CyCLONe) and the computer security incident response teams (CSIRTs) network.

The cross-border SOCs platforms should constitute a new capability that is complementary to the CSIRTs network, by pooling and sharing data on cybersecurity threats from public and

[5] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

[6] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

[7] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

[8] Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM/2022/454 final.

private entities, enhancing the value of such data through expert analysis and state of the art tools, and contributing to the development of Union capabilities and technological sovereignty.

Finally, this proposal is consistent with the Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure[9] that invites Member States to take urgent and effective measures, and to cooperate loyally, efficiently, in solidarity and in a coordinated manner with each other, the Commission and other relevant public authorities as well as the entities concerned, to enhance the resilience of critical infrastructure used to provide essential services in the internal market.

- **Consistency with other Union policies**

The proposal is consistent with other crisis emergency mechanisms and protocols, such as the Integrated Political Crisis Response Mechanism (IPCR). The Cyber Solidarity Act will complement these crisis management frameworks and protocols by providing dedicated support for preparedness and response to cybersecurity incidents. The proposal will also be consistent with the EU's external action in response to large-scale incidents in the framework of the Common Foreign and Security Policy (CFSP), including through the EU Cyber Diplomacy Toolbox. The proposal will complement actions implemented in the context of Article 42(7) of the Treaty on the European Union or in situations defined in Article 222 of the Treaty on the Functioning of the European Union.

It also complements the Union Civil Protection Mechanism (UCPM)[10]established in December 2013 and completed with a new legislation adopted in May 2021[11], that strengthens the prevention, preparedness and response pillars of the UCPM and gives the EU additional capacities to respond to new risks in Europe and the world and boosts the rescEU reserve.

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

- **Legal basis**

The legal basis for this proposal is Article 173(3) and Article 322(1), point (a) of the Treaty on the Functioning of the European Union (TFEU). Article 173 TFEU provides that the Union and the Member States shall ensure that the conditions necessary for the competitiveness of the Union's industry exists. This Regulation aims at strengthening the competitive position of industry and service sectors in Europe across the digitised economy and supporting their digital transformation, by reinforcing the level of cybersecurity in the Digital Single Market. In particular, it aims at increasing the resilience of citizens, businesses and entities operating in

[9] Council Recommendation of 8 December 2022 on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure (Text with EEA relevance) 2023/C 20/01.

[10] Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism (Text with EEA relevance).

[11] Regulation (EU) 2021/836 of the European Parliament and of the Council of 20 May 2021 amending Decision No 1313/2013/EU on a Union Civil Protection Mechanism (Text with EEA relevance).

critical and highly critical sectors against the growing cybersecurity threats, which can have devastating societal and economic impacts.

The proposal is based also on Article 322(1), point (a) TFEU because it contains specific carry-over rules derogating from the principle of annuality set out in Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council (the 'Financial Regulation')[12]. For the purpose of sound financial management and considering the unpredictable, exceptional and specific nature of the cybersecurity landscape and cyber-threats, the Cybersecurity Emergency Mechanism should benefit from a certain degree of flexibility in relation to budgetary management, and in particular by allowing unused commitment and payment appropriations for actions pursuing the objectives set out in the Regulation to be automatically carried over to the following financial year. As this new rule raises issues with the Financial Regulation, this matter could be addressed in the context of the current negotiations of the Financial Regulation recast.

- **Subsidiarity (for non-exclusive competence)**

The strong cross-border nature of cybersecurity threats and the growing number of risks and incidents, which have spill-over effects across borders, sectors, and products, mean that the objectives of the present intervention cannot effectively be achieved by Member States alone and require common action and solidarity at Union level.

The experience of countering cyber-threats stemming from the war against Ukraine, together with the lessons learned from a cybersecurity exercise conducted under the French Presidency (EU CyCLES), showed that concrete mutual support mechanisms, notably cooperation with the private sector, should be developed to achieve solidarity at EU level. Against this background, the Council Conclusions of 23 May 2022 on the development of the European Union's cyber posture calls upon the Commission to present a proposal on a new Emergency Response Fund for Cybersecurity.

Support and actions at Union level to better detect cybersecurity threats, and to increase preparedness and response capacities provide added value because it avoids duplication of efforts across the Union and Member States. It would lead to a better exploitation of existing assets and to greater coordination and exchange of information on lessons learned. The Cyber Emergency Mechanism also envisages providing support to third countries associated to DEP from the EU Cybersecurity Reserve.

The support provided through the various initiatives to be established and funded at Union level will complement and not duplicate national capabilities as regards detection, situational awareness, preparedness and response to cyber threats and incidents.

- **Proportionality**

[12] Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union (OJ L 193, 30.7.2018, p. 1).

The actions do not go beyond what is needed to achieve the general and specific objectives of the Regulation. The actions in this Regulation do not affect Member States' responsibilities for national security, public security, the prevention, investigation, detection, and prosecution of criminal offences. Nor do they affect the legal obligations of entities operating in critical and highly critical sectors to adopt cybersecurity measures, in accordance with the NIS 2 Directive.

The actions covered by this Regulation are complementary to such efforts and measures, by supporting the creation of infrastructures for better detection and analysis of threats and providing support for preparedness and response actions in case of significant or large-scale incidents.

- **Choice of the instrument**

The proposal takes the form of a Regulation of the European Parliament and of the Council. This is the most suitable legal instrument, as only a Regulation, with its directly applicable legal provisions, can provide the necessary degree of uniformity needed for the establishment and operation of a European Cyber Shield and Cyber Emergency Mechanism, by providing for support from DEP for their establishment as well as clear conditions for using and allocating this support.

3. RESULTS OF EX-POST EVALUATIONS, STAKEHOLDER CONSULTATIONS AND IMPACT ASSESSMENTS

- **Stakeholder consultations**

The actions of this Regulation will be supported by DEP, which was subject to wide consultation. In addition, they will build on first steps that have been prepared in close cooperation with the main stakeholders. As regards SOCs, the Commission has developed a concept paper on the development of cross-border SOCs platforms and a Call for Expression of Interest in close cooperation with Member States in the framework of the European Cybersecurity Competence Centre (ECCC). In this context, a survey of national SOCs capacities was conducted and common approaches and technical requirements have been discussed within the technical working group of the ECCC that gathers representatives of Member States. In addition, exchanges took place with industry, notably through the expert group on SOCs created by ENISA and the European Cyber Security Organisation (ECSO).

Secondly, as regards preparedness and incident response, the Commission has set up a short-term programme to support Member States, through additional funding allocated to ENISA from DEP, to immediately reinforce preparedness and capacities to respond to major cyber incidents. Member States' and industry's feedback gathered during the implementation of this short-term programme is already providing valuable insights that have fed into the preparation of the proposed Regulation to address identified shortcomings. This was a first step in line with the Council conclusions on the Cyber posture requesting the Commission to come forward with a proposal for a new Emergency Response Fund for Cybersecurity.

In addition, a workshop with Member States experts on the Cyber Emergency Mechanism was held on 16 February 2023, on the basis of a discussion paper. All Member States participated in this workshop and eleven Member States provided further contributions in writing.

- **Impact assessment**

Due to the urgent nature of the proposal, no impact assessment was carried out. The actions of this Regulation will be supported by the DEP and are in line with those set in the DEP Regulation, which was subject to a dedicated impact assessment. This Regulation will not entail any significant administrative or environmental impacts beyond those already assessed in the impact assessment of the DEP Regulation.

Furthermore, it builds on first actions developed in closed collaboration with the main stakeholders, as set out above, and follow up on Member States' call for the Commission to present a proposal on a new Emergency Response Fund for Cybersecurity by the end of Q3 2022.

Specifically, regarding situational awareness and detection under the European Cyber Shield, a Call for Expression of Interest to jointly procure tools and infrastructure to establish Cross-border SOCs, and a call for grants to enable capacity building of SOCs serving public and private organisations, were held under DEP cybersecurity work programme 2021-2022.

In the area of preparedness and incident response, as mentioned above the Commission has set up a short-term programme to support Member States from DEP, being implemented by ENISA. Services covered include preparedness actions, such as penetration testing of critical entities in order to identify vulnerabilities. It also strengthens possibilities to assist Member States in case of a major incident affecting critical entities. The implementation by ENISA of this short-term programme is under way and has already provided relevant insights that have been taken into account in the preparation of this Regulation.

- **Fundamental rights**

By contributing to the security of digital information, this proposal will contribute to protecting the right to liberty and security in accordance with Article 6 of the EU Charter of Fundamental Rights, and the right to respect for private and family life in accordance with Article 7 of the EU Charter of Fundamental Rights. By protecting businesses from economically damaging cyberattacks, the proposal will also contribute to the freedom to conduct a business in accordance with Article 16 of the EU Charter of Fundamental Rights, and the right to property in accordance with Article 17 of the EU Charter of Fundamental Rights. Finally, by protecting the integrity of critical infrastructure in the face of cyberattacks, the proposal will contribute to the right to healthcare in accordance with Article 35 of the EU Charter of Fundamental Rights, and the right to access to services of general economic interest in accordance with Article 36 of the EU Charter of Fundamental Rights.

4. BUDGETARY IMPLICATIONS

The actions of this Regulation will be supported by funding under Strategic Objective 'Cybersecurity' of DEP.

The total budget includes an increase of EUR 100 million that this Regulation proposes to re-allocate from other Strategic Objectives of DEP. This will bring the new total amount available for Cybersecurity actions under DEP to EUR 842.8 million.

Part of the additional EUR 100 million will reinforce the budget managed by the ECCC to implement actions on SOCs and preparedness as part of their Work Programme(s). Moreover, the additional funding will serve to support the establishment of the EU Cybersecurity Reserve.

It complements the budget already foreseen for similar actions in the main DEP and Cybersecurity DEP WP from the period 2023-2027 which could bring the total amount to 551 million for 2023-2027, while 115 million were dedicated already in the form of pilots for 2021-2022. Including Member States contributions, the overall budget could amount up to 1.109 billion euros.

An overview of the costs involved is included in the 'Legislative financial statement' accompanying this proposal.

5. OTHER ELEMENTS

- **Implementation plans and monitoring, evaluation and reporting arrangements**

The Commission will monitor the implementation, the application, and the compliance with these new provisions with a view to assessing their effectiveness. The Commission shall submit a report on the evaluation and review of this Regulation to the European Parliament and to the Council by four years after the date of its application.

- **Detailed explanation of the specific provisions of the proposal**

General Objectives, subject matter, and definitions (Chapter I)

Chapter I sets out the objectives of the Regulation to strengthen solidarity at Union level in order to better detect, prepare and respond to cybersecurity threats and incidents and in particular, to strengthen common Union detection and situational awareness of cyber threats and incidents, to 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 and to enhance Union resilience by reviewing and assessing significant or large-scaleincidents. This Chapter also sets out the actions through which these objectives will be achieved: the deployment of a European Cyber Shield, the creation of a Cyber Emergency Mechanism and the establishment of a Cybersecurity Incident Review Mechanism. It also sets out the definitions used throughout the instrument.

The European Cyber Shield (Chapter II)

Chapter II establishes the European Cyber Shield and sets out its various elements and the conditions for participation. Firstly, it announces the overall objective of the European Cyber Shield, which is to develop advanced capabilities for the Union to detect, analyse and process data on cyber threats and incidents in the Union, as well as the specific operational objectives. It specifies that Union funding for the European Cyber Shield shall be implemented in accordance with the DEP Regulation.

Further, the chapter describes the type of entities that shall form the European Cyber Shield. The shield shall consist of National Security Operations Centres ('National SOCs') and Cross-border Security Operations Centres ('Cross-border SOCs'). A National SOC shall be designated by each participating Member State. This shall 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. Following a Call for Expression of Interest, a National SOC may be selected by the ECCC to participate in a joint procurement of tools and infrastructures with the ECCC and to receive a grant for running the tools and infrastructures. If a National SOC benefits from Union support, it shall commit to apply participate in a Cross-border SOC within two years.

Cross-border SOCs shall consist of a consortium of at least three Member States, represented by National SOCs, who are committed to work together to coordinate their cyber detection and threat monitoring activities. Following an initial Call for Expression of Interest, a Hosting Consortium may be selected by the ECCC to participate in a joint procurement of tools and infrastructures with the ECCC and to receive a grant for running the tools and infrastructures. Members of the Hosting Consortium shall conclude a written consortium agreement which sets out their internal arrangements. This chapter then details the requirements for sharing information among the participants in a Cross-border SOC, and for sharing information between a Cross-border SOC and other Cross-border SOCs, as well as with relevant EU entities. National SOCs participating in a Cross-border SOC shall share relevant cyber threat related information with one another, and the details, including the commitment to share significant amount of data and the conditions thereof should be defined in a consortium agreement. Cross-border SOCs shall ensure a high-level of interoperability between themselves. Cross-border SOCs should also conclude cooperation agreements with other Cross-border SOCs, specifying information sharing principles. Where Cross-border SOCs obtain information relating to a potential or ongoing large-scale cybersecurity incident, they shall provide relevant information to EU CyCLONe, the CSIRTs network and the Commission, in view of their respective crisis management roles in accordance with Directive (EU) 2022/2555. Chapter II concludes by specifying the security conditions for participating in the European Cyber Shield.

Cybersecurity Emergency Mechanism (Chapter III)

Chapter III establishes the Cyber Emergency Mechanism to improve the Union's resilience to major cybersecurity threats and prepare for and mitigate, in a spirit of solidarity, the short-term impact of significant and large-scale cybersecurity incidents or crises. Actions implementing the Cyber Emergency Mechanism shall be supported by funding from DEP. The Mechanism provides for actions to support preparedness, including coordinated testing of entities operating

in highly critical sectors, response to and immediate recovery from significant or large-scale cybersecurity incidents or mitigate significant cyber threats and mutual assistance actions.

The Cyber Emergency Mechanism preparedness actions include the coordinated preparedness testing of entities operating in highly critical sectors. The Commission, after consulting ENISA and the NIS Cooperation Group, should regularly identify relevant sectors or subsectors from the Sectors of High Criticality listed in Annex I of Directive (EU) No 2022/2555, from which entities may be subject to the coordinated preparedness testing at EU level.

For the purpose of implementing the proposed incident response actions, this Regulation establishes an EU Cybersecurity Reserve, consisting of incident response services from trusted providers, selected in accordance with the criteria laid down in this Regulation. Users of the services from the EU Cybersecurity Reserve shall include Member States' cyber crisis management authorities and CSIRTs and Union institutions, bodies and agencies. The Commission shall have overall responsibility for the implementation of the EU Cybersecurity Reserve and may entrust, in full or in part, ENISA with the operation and administration of the EU Cybersecurity Reserve.

To receive support from the EU Cybersecurity Reserve, the users should take their own measures to mitigate the effects of the incident for which the support is requested. The requests for support from the EU Cybersecurity Reserve should include necessary relevant information about the incident and the measures already taken by the users. The Chapter describes as well the implementation modalities, including assessment of requests to the EU Cybersecurity Reserve.

The Regulation provides as well for the procurement principles and selection criteria regarding trusted providers of the EU Cybersecurity Reserve.

Third countries may request support from the EU Cybersecurity Reserve where Association Agreements concluded regarding their participation in DEP provide for this. This Chapter describes further conditions and modalities of such participation.

Cybersecurity Incident Review Mechanism (Chapter IV)

At the request of the Commission, the EU-CyCLONe or the CSIRTs network, ENISA should review and assess threats, vulnerabilities and mitigation actions with respect to a specific significant or large-scale cybersecurity incident. The review and assessment should be delivered by ENISA in the form of an incident review report to the CSIRTs network, the EU-CyCLONe and the Commission to support them in carrying out their tasks. When the incident relates to a third country, the report should be shared by the Commission with the High Representative. The report should include lessons learned and where appropriate, recommendations to improve the Union's cyber posture.

Final Provisions (Chapter V)

Chapter V contains amendments to the DEP Regulation, and an obligation for the Commission to prepare regular reports for the evaluation and review of the Regulation to the European Parliament and to the Council. The Commission is empowered to adopt implementing acts in accordance with the examination procedure referred to in Article 21 to: specify the conditions for this interoperability between Cross-border SOCs; determine the procedural arrangements for the information sharing related to a potential or ongoing large-scale cybersecurity incident between Cross-border SOCs and Union entities; laying down technical requirements to ensure a high level of data and physical security of the infrastructure and to protect the security interests of the Union when sharing information with entities that are not Member States public bodies; specify the types and the number of response services required for the EU Cybersecurity Reserve; and, specify further the detailed arrangements for allocating the EU Cybersecurity Reserve support services.

2023/0109 (COD)

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

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 173(3) and Article 322(1), point (a) thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the Court of Auditors[1]

Having regard to the opinion of the European Economic and Social Committee[2],

Having regard to the opinion of the Committee of the Regions[3],

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) The use of and dependence on information and communication technologies have become fundamental aspects in all sectors of economic activity as our public administrations, companies and citizens are more interconnected and interdependent across sectors and borders than ever before.

(2) The magnitude, frequency and impact of cybersecurity incidents are increasing, including supply chain attacks aiming at cyberespionage, ransomware or disruption. They represent a major threat to the functioning of network and information systems. In view of the fast-evolving threat landscape, the threat of possible large-scale incidents causing significant disruption or damage to critical infrastructures demands heightened preparedness at all levels of the Union's cybersecurity framework. That threat goes beyond Russia's military aggression on Ukraine, and is likely to persist given the multiplicity of state-aligned, criminal and hacktivist actors involved in current geopolitical tensions. Such incidents can impede the provision of public services and the pursuit of economic activities, including in critical or highly critical sectors, generate substantial financial losses, undermine user confidence, cause major damage to the economy of the Union, and could even have health or life-threatening consequences. Moreover, cybersecurity incidents are unpredictable, as they often emerge and evolve within very short periods of time, not contained within any specific geographical area, and occurring simultaneously or spreading instantly across many countries.

(3) It is necessary to strengthen the competitive position of industry and services sectors in the Union across the digitised economy and support their digital transformation, by

[1] OJ C […], […], p. […].
[2] OJ C , , p. .
[3] OJ C , , p. .

reinforcing the level of cybersecurity in the Digital Single Market. As recommended in three different proposals of the Conference on the Future of Europe[4] , it is necessary to increase the resilience of citizens, businesses and entities operating critical infrastructures against the growing cybersecurity threats, which can have devastating societal and economic impacts. Therefore, investment in infrastructures and services that will support faster detection and response to cybersecurity threats and incidents is needed, and Member States need assistance in better preparing for, as well as responding to significant and large-scale cybersecurity incidents. The Union should also increase its capacities in these areas, notably as regards the collection and analysis of data on cybersecurity threats and incidents.

(4) The Union has already taken a number of measures to reduce vulnerabilities and increase the resilience of critical infrastructures and entities against cybersecurity risks, in particular Directive (EU) 2022/2555 of the European Parliament and of the Council[5], Commission Recommendation (EU) 2017/1584[6], Directive 2013/40/EU of the European Parliament and of the Council[7] and Regulation (EU) 2019/881 of the European Parliament and of the Council[8]. In addition, the Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure invites Member States to take urgent and effective measures, and to cooperate loyally, efficiently, in solidarity and in a coordinated manner with each other, the Commission and other relevant public authorities as well as the entities concerned, to enhance the resilience of critical infrastructure used to provide essential services in the internal market.

(5) The growing cybersecurity risks and an overall complex threat landscape, with a clear risk of rapid spill-over of cyber incidents from one Member State to others and from a third country to the Union requires strengthened solidarity at Union level to better detect, prepare for and respond to cybersecurity threats and incidents. Member States have also invited the Commission to present a proposal on a new Emergency Response Fund for Cybersecurity in the Council Conclusions on an EU Cyber Posture[9].

(6) The Joint Communication on the EU Policy on Cyber Defence[10] adopted on 10 November 2022 announced an EU Cyber Solidarity Initiative with the following objectives: strengthening of common EU detection, situational awareness and response capabilities by promoting the deployment of an EU infrastructure of Security Operations Centres (‘SOCs’), supporting gradual building of an EU-level cybersecurity reserve

---

4 https://futureu.europa.eu/en/

5 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (OJ L 333, 27.12.2022).

6 Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises (OJ L 239, 19.9.2017, p. 36).

7 Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (J L 218, 14.8.2013, p. 8).

8 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15).

9 Council conclusions on the development of the European Union's cyber posture approved by the Council at its meeting on 23 May 2022, (9364/22)

10 Join Communication to the European Parliament and the Council EU Policy on Cyber Defence JOIN/2022/49 final

with services from trusted private providers and testing of critical entities for potential vulnerabilities based on EU risk assessments.

(7) It is necessary to strengthen the detection and situational awareness of cyber threats and incidents throughout the Union and to strengthen solidarity by enhancing Member States' and the Union's preparedness and capabilities to respond to significant and large-scale cybersecurity incidents. Therefore a pan-European infrastructure of SOCs (European Cyber Shield) should be deployed to build and enhance common detection and situational awareness capabilities; a Cybersecurity Emergency Mechanism should be established to support Member States in preparing for, responding to, and immediately recovering from significant and large-scale cybersecurity incidents; a Cybersecurity Incident Review Mechanism should be established to review and assess specific significant or large-scale incidents. These actions shall be without prejudice to Articles 107 and 108 of the Treaty on the Functioning of the European Union ('TFEU').

(8) To achieve these objectives, it is also necessary to amend Regulation (EU) 2021/694 of the European Parliament and of the Council[11] in certain areas. In particular, this Regulation should amend Regulation (EU) 2021/694 as regards adding new operational objectives related to the European Cyber Shield and the Cyber Emergency Mechanism under Specific Objective 3 of DEP, which aims at guaranteeing the resilience, integrity and trustworthiness of the Digital Single Market, at strengthening capacities to monitor cyber-attacks and threats and to respond to them, and at reinforcing cross-border cooperation on cybersecurity. This will be complemented by the specific conditions under which financial support may be granted for those actions should be established and the governance and coordination mechanisms necessary in order to achieve the intended objectives should be defined. Other amendments to Regulation (EU) 2021/694 should include descriptions of proposed actions under the new operational objectives, as well as measurable indicators to monitor the implementation of these new operational objectives.

(9) The financing of actions under this Regulation should be provided for in Regulation (EU) 2021/694, which should remain the relevant basic act for these actions enshrined within the Specific Objective 3 of DEP. Specific conditions for participation concerning each action will be provided for in the relevant work programmes, in line with the applicable provision of Regulation (EU) 2021/694.

(10) Horizontal financial rules adopted by the European Parliament and by the Council on the basis of Article 322 TFEU apply to this Regulation. Those rules are laid down in the Financial Regulation and determine in particular the procedure for establishing and implementing the Union budget, and provide for checks on the responsibility of financial actors. Rules adopted on the basis of Article 322 TFEU also include a general regime of conditionality for the protection of the Union budget as established in Regulation (EU, Euratom) 2020/2092 of the European Parliament and of the Council.

(11) For the purpose of sound financial management, specific rules should be laid down for the carry-over of unused commitment and payment appropriations. While respecting the principle that the Union budget is set annually, this Regulation should, on account of the unpredictable, exceptional and specific nature of the cybersecurity landscape, provide for possibilities to carry over unused funds beyond those set out in the Financial

[11] Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240 (OJ L 166, 11.5.2021, p. 1).

Regulation, thus maximising the Cybersecurity Emergency Mechanism's capacity to support Member States in countering effectively cyber threats.

(12) To more effectively prevent, assess and respond to cyber threats and incidents, it is necessary to develop more comprehensive knowledge about the threats to critical assets and infrastructures on the territory of the Union, including their geographical distribution, interconnection and potential effects in case of cyber-attacks affecting those infrastructures. A large-scale Union infrastructure of SOCs should be deployed ('the European Cyber Shield'), comprising of several interoperating cross-border platforms, each grouping together several National SOCs. That infrastructure should serve national and Union cybersecurity interests and needs, leveraging state of the art technology for advanced data collection and analytics tools, enhancing cyber detection and management capabilities and providing real-time situational awareness. That infrastructure should serve to increase detection of cybersecurity threats and incidents and thus complement and support Union entities and networks responsible for crisis management in the Union, notably the EU Cyber Crises Liaison Organisation Network ('EU-CyCLONe'), as defined in Directive (EU) 2022/2555 of the European Parliament and of the Council[12].

(13) Each Member State should designate a public body at national level tasked with coordinating cyber threat detection activities in that Member State. These National SOCs should act as a reference point and gateway at national level for participation in the European Cyber Shield and should ensure that cyber threat information from public and private entities is shared and collected at national level in an effective and streamlined manner.

(14) As part of the European Cyber Shield, a number of Cross-border Cybersecurity Operations Centres ('Cross-border SOCs') should be established. These should bring together National SOCs from at least three Member States, so that the benefits of cross-border threat detection and information sharing and management can be fully achieved. The general objective of Cross-border SOCs should be to strengthen capacities to analyse, prevent and detect cybersecurity threats and to support the production of high-quality intelligence on cybersecurity threats, notably through the sharing of data from various sources, public or private, as well as through the sharing and joint use of state-of-the-art tools, and jointly developing detection, analysis and prevention capabilities in a trusted environment. They should provide new additional capacity, building upon and complementing existing SOCs and computer incident response teams ('CSIRTs') and other relevant actors.

(15) At national level, the monitoring, detection and analysis of cyber threats is typically ensured by SOCs of public and private entities, in combination with CSIRTs. In addition, CSIRTs exchange information in the context of the CSIRT network, in accordance with Directive (EU) 2022/2555. The Cross-border SOCs should constitute a new capability that is complementary to the CSIRTs network, by pooling and sharing data on cybersecurity threats from public and private entities, enhancing the value of such data through expert analysis and jointly acquired infrastructures and state of the art tools, and contributing to the development of Union capabilities and technological sovereignty.

---

[12] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80).

(16) The Cross-border SOCs should act as a central point allowing for a broad pooling of relevant data and cyber threat intelligence, enable the spreading of threat information among a large and diverse set of actors (e.g., Computer Emergency Response Teams ('CERTs'), CSIRTs, Information Sharing and Analysis Centers ('ISACs'), operators of critical infrastructures). The information exchanged among participants in a Cross-border SOC could include data from networks and sensors, threat intelligence feeds, indicators of compromise, and contextualised information about incidents, threats and vulnerabilities. In addition, Cross-border SOCs should also enter into cooperation agreements with other Cross-border SOCs.

(17) Shared situational awareness among relevant authorities is an indispensable prerequisite for Union-wide preparedness and coordination with regards to significant and large-scale cybersecurity incidents. Directive (EU) 2022/2555 establishes the EU–CyCLONe to support the coordinated management of large-scale cybersecurity incidents and crises at operational level and to ensure the regular exchange of relevant information among Member States and Union institutions, bodies and agencies. Recommendation (EU) 2017/1584 on coordinated response to large-scale cybersecurity incidents and crises addresses the role of all relevant actors. Directive (EU) 2022/2555 also recalls the Commission's responsibilities in the Union Civil Protection Mechanism ('UCPM') established by Decision 1313/2013/EU of the European Parliament and of the Council, as well as for providing analytical reports for the Integrated Political Crisis Response Mechanism ('IPCR') arrangements under Implementing Decision (EU) 2018/1993. Therefore, in situations where Cross-border SOCs obtain information related to a potential or ongoing large-scale cybersecurity incident, they should provide relevant information to EU-CyCLONe, the CSIRTs network and the Commission. In particular, depending on the situation, information to be shared could include technical information, information about the nature and motives of the attacker or potential attacker, and higher-level non-technical information about a potential or ongoing large-scale cybersecurity incident. In this context, due regard should be paid to the need-to-know principle and to the potentially sensitive nature of the information shared.

(18) Entities participating in the European Cyber Shield should ensure a high-level of interoperability among themselves including, as appropriate, as regards data formats, taxonomy, data handling and data analysis tools, and secure communications channels, a minimum level of application layer security, situational awareness dashboard, and indicators. The adoption of a common taxonomy and the development of a template for situational reports to describe the technical cause and impacts of cybersecurity incidents should take into account the ongoing work on incident notification in the context of the implementation of Directive (EU) 2022/2555.

(19) In order to enable the exchange of data on cybersecurity threats from various sources, on a large-scale basis, in a trusted environment, entities participating in the European Cyber Shield should be equipped with state-of-the-art and highly-secure tools, equipment and infrastructures. This should make it possible to improve collective detection capacities and timely warnings to authorities and relevant entities, notably by using the latest artificial intelligence and data analytics technologies.

(20) By collecting, sharing and exchanging data, the European Cyber Shield should enhance the Union's technological sovereignty. The pooling of high-quality curated data should also contribute to the development of advanced artificial intelligence and data analytics technologies. It should be facilitated through the connection of the European Cyber

Shield with the pan-European High Performance Computing infrastructure established by Council Regulation (EU) 2021/1173[13].

(21) While the European Cyber Shield is a civilian project, the cyber defence community could benefit from stronger civilian detection and situational awareness capabilities developed for the protection of critical infrastructure. Cross-border SOCs, with the support of the Commission and the European Cybersecurity Competence Centre ('ECCC'), and in cooperation with the High Representative of the Union for Foreign Affairs and Security Policy (the 'High Representative'), should gradually develop dedicated protocols and standards to allow for cooperation with the cyber defence community, including vetting and security conditions. The development of the European Cyber Shield should be accompanied by a reflection enabling future collaboration with networks and platforms responsible for information sharing in the cyber defence community, in close cooperation with the High Representative.

(22) Information sharing among participants of the European Cyber Shield should comply with existing legal requirements and in particular Union and national data protection law, as well as the Union rules on competition governing the exchange of information. The recipient of the information should implement, insofar as the processing of personal data is necessary, technical and organisational measures that safeguard the rights and freedoms of data subjects, and destroy the data as soon as they are no longer necessary for the stated purpose and inform the body making the data available that the data have been destroyed.

(23) Without prejudice to Article 346 of TFEU, the exchange of information that is confidential pursuant to Union or national rules should be limited to that which is relevant and proportionate to the purpose of that exchange. The exchange of such information should preserve the confidentiality of the information and protect the security and commercial interests of the entities concerned, in full respect of trade and business secrets.

(24) In view of the increasing risks and number of cyber incidents affecting Member States, it is necessary to set up a crisis support instrument to improve the Union's resilience to significant and large-scale cybersecurity incidents and complement Member States' actions through emergency financial support for preparedness, response and immediate recovery of essential services. That instrument should enable the rapid deployment of assistance in defined circumstances and under clear conditions and allow for a careful monitoring and evaluation of how resources have been used. Whilst the primary responsibility for preventing, preparing for and responding to cybersecurity incidents and crises lies with the Member States, the Cyber Emergency Mechanism promotes solidarity between Member States in accordance with Article 3(3) of the Treaty on European Union ('TEU').

(25) The Cyber Emergency Mechanism should provide support to Member States complementing their own measures and resources, and other existing support options in case of response to and immediate recovery from significant and large-scale cybersecurity incidents, such as the services provided by the European Union Agency for Cybersecurity ('ENISA') in accordance with its mandate, the coordinated response and the assistance from the CSIRTs network, the mitigation support from the EU-CyCLONe, as well as mutual assistance between Member States including in the context

[13] Council Regulation (EU) 2021/1173 of 13 July 2021 on establishing the European High Performance Computing Joint Undertaking and repealing Regulation (EU) 2018/1488 (OJ L 256, 19.7.2021, p. 3).

of Article 42(7) of TEU, the PESCO Cyber Rapid Response Teams[14] and Hybrid Rapid Response Teams. It should address the need to ensure that specialised means are available to support preparedness and response to cybersecurity incidents across the Union and in third countries.

(26) This instrument is without prejudice to procedures and frameworks to coordinate crisis response at Union level, in particular the UCPM[15], IPCR[16,] and Directive (EU) 2022/2555. It may contribute to or complement actions implemented in the context of Article 42(7) of TEU or in situations defined in Article 222 of TFEU. The use of this instrument should also be coordinated with the implementation of Cyber Diplomacy Toolbox's measures, where appropriate.

(27) Assistance provided under this Regulation should be in support of, and complementary to, the actions taken by Member States at national level. To this end, close cooperation and consultation between the Commission and the affected Member State should be ensured. When requesting support under the Cyber Emergency Mechanism, the Member State should provide relevant information justifying the need for support.

(28) Directive (EU) 2022/2555 requires Member States to designate or establish one or more cyber crisis management authorities and ensure they have adequate resources to carry out their tasks in an effective and efficient manner. It also requires Member States to identify capabilities, assets and procedures that can be deployed in the case of a crisis as well as to adopt a national large-scale cybersecurity incident and crisis response plan where the objectives of and arrangements for the management of large-scale cybersecurity incidents and crises are set out. Member States are also required to establish one or more CSIRTs tasked with incident handling responsibilities in accordance with a well-defined process and covering at least the sectors, subsectors and types of entities under the scope of that Directive, and to ensure they have adequate resources to carry out effectively their tasks. This Regulation is without prejudice to the Commission's role in ensuring the compliance by Member States with the obligations of Directive (EU) 2022/2555. The Cyber Emergency Mechanism should provide assistance for actions aimed at reinforcing preparedness as well as incident response actions to mitigate the impact of significant and large-scale cybersecurity incidents, to support immediate recovery and/or restore the functioning of essential services.

(29) As part of the preparedness actions, to promote a consistent approach and strengthen security across the Union and its internal market, support should be provided for testing and assessing cybersecurity of entities operating in highly critical sectors identified pursuant to Directive (EU) 2022/2555 in a coordinated manner. For this purpose, the Commission, with the support of ENISA and in cooperation with the NIS Cooperation Group established by Directive (EU) 2022/2555, should regularly identify relevant sectors or subsectors, which should be eligible to receive financial support for coordinated testing at Union level. The sectors or subsectors should be selected from Annex I to Directive (EU) 2022/2555 ('Sectors of High Criticality'). The coordinated testing exercises should be based on common risk scenarios and methodologies. The selection of sectors and development of risk scenarios should take into account relevant

---

14 COUNCIL DECISION (CFSP) 2017/ 2315 - of 11 December 2017 - establishing permanent structured cooperation (PESCO) and determining the list of participating Member States.

15 Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism (OJ L 347, 20.12.2013, p. 924).

16 Integrated Political Crisis Response arrangements (IPCR) and in accordance with Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises.

Union-wide risk assessments and risk scenarios, including the need to avoid duplication, such as the risk evaluation and risk scenarios called for in the Council conclusions on the development of the European Union's cyber posture to be conducted by the Commission, the High Representative and the NIS Cooperation Group, in coordination with relevant civilian and military bodies and agencies and established networks, including the EU CyCLONe, as well as the risk assessment of communications networks and infrastructures requested by the Joint Ministerial Call of Nevers and conducted by the NIS Cooperation Group, with the support of the Commission and ENISA, and in cooperation with the Body of European Regulators for Electronic Communications (BEREC), the coordinated risk assessments to be conducted under Article 22 of Directive (EU) 2022/2555 and digital operational resilience testing as provided for in Regulation (EU) 2022/2554 of the European Parliament and of the Council[17]. The selection of sectors should also take into account the Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure.

(30) In addition, the Cyber Emergency Mechanism should offer support for other preparedness actions and support preparedness in other sectors, not covered by the coordinated testing of entities operating in highly critical sectors. Those actions could include various types of national preparedness activities.

(31) The Cyber Emergency Mechanism should also provide support for incident response actions to mitigate the impact of significant and large-scale cybersecurity incidents, to support immediate recovery or restore the functioning of essential services. Where appropriate, it should complement the UCPM to ensure a comprehensive approach to respond to the impacts of cyber incidents on citizens.

(32) The Cyber Emergency Mechanism should support assistance provided by Member States to a Member State affected by a significant or large-scale cybersecurity incident, including by the CSIRTs network set out in Article 15 of Directive (EU) 2022/2555. Member States providing assistance should be allowed to submit requests to cover costs related to dispatching of expert teams in the framework of mutual assistance. The eligible costs could include travel, accommodation and daily allowance expenses of cybersecurity experts.

(33) A Union-level Cybersecurity Reserve should gradually be set up, consisting of services from private providers of managed security services to support response and immediate recovery actions in cases of significant or large-scale cybersecurity incidents. The EU Cybersecurity Reserve should ensure the availability and readiness of services. The services from the EU Cybersecurity Reserve should serve to support national authorities in providing assistance to affected entities operating in critical or highly critical sectors as a complement to their own actions at national level. When requesting support from the EU Cybersecurity Reserve, Member States should specify the support provided to the affected entity at the national level, which should be taken into account when assessing the Member State request. The services from the EU Cybersecurity Reserve may also serve to support Union institutions, bodies and agencies, under similar conditions.

(34) For the purpose of selecting private service providers to provide services in the context of the EU Cybersecurity Reserve, it is necessary to establish a set of minimum criteria that should be included in the call for tenders to select these providers, so as to ensure

[17] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011

that the needs of Member States' authorities and entities operating in critical or highly critical sectors are met.

(35) To support the establishment of the EU Cybersecurity Reserve, the Commission could consider requesting ENISA to prepare a candidate certification scheme pursuant to Regulation (EU) 2019/881 for managed security services in the areas covered by the Cyber Emergency Mechanism.

(36) In order to support the objectives of this Regulation of promoting shared situational awareness, enhancing Union's resilience and enabling effective response to significant and large-scale cybersecurity incidents, the EU=CyCLONe, the CSIRTs network or the Commission should be able to ask ENISA to review and assess threats, vulnerabilities and mitigation actions with respect to a specific significant or large-scale cybersecurity incident. After the completion of a review and assessment of an incident, ENISA should prepare an incident review report, in collaboration with relevant stakeholders, including representatives from the private sector, Member States, the Commission and other relevant EU institutions, bodies and agencies. As regards the private sector, ENISA is developing channels for exchanging information with specialised providers, including providers of managed security solutions and vendors, in order to contribute to ENISA's mission of achieving a high common level of cybersecurity across the Union. Building on the collaboration with stakeholders, including the private sector, the review report on specific incidents should aim at assessing the causes, impacts and mitigations of an incident, after it has occurred. Particular attention should be paid to the input and lessons shared by the managed security service providers that fulfil the conditions of highest professional integrity, impartiality and requisite technical expertise as required by this Regulation. The report should be delivered and feed into the work of the EU=CyCLONe, the CSIRTs network and the Commission. When the incident relates to a third country, it will also be shared by the Commission with the High Representative.

(37) Taking into account the unpredictable nature of cybersecurity attacks and the fact that they are often not contained in a specific geographical area and pose high risk of spill-over, the strengthening of resilience of neighbouring countries and their capacity to respond effectively to significant and large-scale cybersecurity incidents contributes to the protection of the Union as a whole. Therefore, third countries associated to the DEP may be supported from the EU Cybersecurity Reserve, where this is provided for in the respective association agreement to DEP. The funding for associated third countries should be supported by the Union in the framework of relevant partnerships and funding instruments for those countries. The support should cover services in the area of response to and immediate recovery from significant or large-scale cybersecurity incidents. The conditions set for the EU Cybersecurity Reserve and trusted providers in this Regulation should apply when providing support to the third countries associated to DEP.

(38) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission to specify the conditions for the interoperability between Cross-border SOCs; determine the procedural arrangements for the information sharing related to a potential or ongoing large-scale cybersecurity incident between Cross-border SOCs and Union entities; laying down technical requirements to ensure security of the European Cyber Shield; specify the types and the number of response services required for the EU Cybersecurity Reserve; and, specify further the detailed arrangements for allocating the EU Cybersecurity Reserve support services. Those powers should be exercised in accordance with Regulation (EU) 182/2011 of the European Parliament and of the Council.

(39) The objective of this Regulation can be better achieved at Union level than by the Member States. Hence, the Union may adopt measures, in accordance with the principles of subsidiarity and proportionality as set out in Article 5 of the Treaty on European Union. This Regulation does not go beyond what is necessary in order to achieve that objective.

HAVE ADOPTED THIS REGULATION:

Chapter I

GENERAL OBJECTIVES, SUBJECT MATTER, AND DEFINITIONS

Article 1

Subject-matter and objectives

1. This Regulation lays down measures to strengthen capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents, in particular through the following actions:

(a) the deployment of a pan-European infrastructure of Security Operations Centres ('European Cyber Shield') to build and enhance common detection and situational awareness capabilities;

(b) the creation of a Cybersecurity Emergency Mechanism to support Member States in preparing for, responding to, and immediate recovery from significant and large-scale cybersecurity incidents;

(c) the establishment of a European Cybersecurity Incident Review Mechanism to review and assess significant or large-scale incidents.

2. This Regulation pursues the objective to strengthen solidarity at Union level through following specific objectives:

(a) to 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;

(b) to 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');

(c) to 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..

3. This Regulation is without prejudice to the Member States' primary responsibility for national security, public security, and the prevention, investigation, detection and prosecution of criminal offences.

Article 2

Definitions

For the purposes of this Regulation, the following definitions apply:

(1) **'Cross-border Security Operations Centre' ("Cross-border SOC")** means 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**;**

(2) **'public body'** means a body governed by public law as defined in Article 2((1), point (4),), of Directive 2014/24/EU of the European Parliament and the Council[18];

(3) **'Hosting Consortium'** means a consortium composed of participating states, represented by National SOCs, that have agreed to establish and contribute to the acquisition of tools and infrastructure for, and operation of, a Cross-border SOC ;

(4) '**entity'** means an entity as defined in Article 6, point (38), of Directive (EU) 2022/2555*;*

(5) '**entities operating in critical or highly critical sectors'** means type of entities listed in Annex I and Annex II of Directive (EU) 2022/2555;

(6) '**cyber threat'** means a cyber threat as defined in Article 2, point (8), of Regulation (EU) 2019/881;

(7) '**significant cybersecurity incident'** means a cybersecurity incident fulfilling criteria set out in Article 23(3) of Directive (EU) 2022/2555;

(8) '**large-scale cybersecurity incident'** means an incident as defined in Article 6, point (7) of Directive (EU)2022/2555;

(9) **'preparedness'** means a state of readiness and capability to ensure an effective rapid response to a significant or large-scale cybersecurity incident, obtained as a result of risk assessment and monitoring actions taken in advance;

(10) **'response'** means action in the event of a significant or large-scale cybersecurity incident, or during or after such an incident, to address its immediate and short-term adverse consequences;

[18] Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC (OJ L 94 28.3.2014, p. 65).

(11) **'trusted providers'** means managed security service providers as defined in Article 6, point (40), of Directive (EU) 2022/2555 selected in accordance with Article 16 of this Regulation.

Chapter II

THE EUROPEAN CYBER SHIELD

Article 3

Establishment of the European Cyber Shield

1. An interconnected pan-European infrastructure of Security Operations Centres ('European Cyber Shield') shall be established to develop advanced capabilities for the Union to detect, analyse and process data on cyber threats and incidents in the Union. It shall consist of all National Security Operations Centres ('National SOCs') and Cross-border Security Operations Centres ('Cross-border SOCs').

Actions implementing the European Cyber Shield shall be supported by funding from the Digital Europe Programme and implemented in accordance with Regulation (EU) 2021/694 and in particular Specific Objective 3 thereof.

2. The European Cyber Shield shall:

(a) pool and share data on cyber threats and incidents from various sources through cross-border SOCs;

(b) 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;

(c) contribute to better protection and response to cyber threats;

(d) contribute to faster detection of cyber threats and situational awareness across the Union;

(e) provide services and activities for the cybersecurity community in the Union, including contributing to the development advanced artificial intelligence and data analytics tools.

It shall be developed in cooperation with the pan-European High Performance Computing infrastructure established pursuant to Regulation (EU) 2021/1173.

Article 4

National Security Operations Centres

1. In order to participate in the European Cyber Shield, each Member State shall designate at least one National SOC. The National SOC shall be a public body.

It shall 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. It shall be equipped with state-of-the-art technologies capable of detecting, aggregating, and analysing data relevant to cybersecurity threats and incidents.

2. Following a call for expression of interest, National SOCs shall be selected by the European Cybersecurity Competence Centre ('ECCC') to participate in a joint procurement of tools and infrastructures with the ECCC. The ECCC may award grants to the selected National SOCs to fund the operation of those tools and infrastructures. The Union financial contribution shall cover up to 50% of the acquisition costs of the tools and infrastructures, and up to 50% of the operation costs, with the remaining costs to be covered by the Member State. Before launching the procedure for the acquisition of the tools and infrastructures, the ECCC and the National SOC shall conclude a hosting and usage agreement regulating the usage of the tools and infrastructures.

3. A National SOC selected pursuant to paragraph 2 shall 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. If a National SOC is not a participant in a Cross-border SOC by that time, it shall not be eligible for additional Union support under this Regulation.

Article 5

Cross-border Security Operations Centres

1. A 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 shall be eligible to participate in actions to establish a Cross-border SOC.

2. Following a call for expression of interest, a Hosting Consortium shall be selected by the ECCC to participate in a joint procurement of tools and infrastructures with the ECCC. The ECCC may award to the Hosting Consortium a grant to fund the operation of the tools and infrastructures. The Union financial contribution shall cover up to 75% of the acquisition costs of the tools and infrastructures, and up to 50% of the operation costs, with the remaining costs to be covered by the Hosting Consortium. Before launching the procedure for the acquisition of the tools and infrastructures, the ECCC and the Hosting Consortium shall conclude a hosting and usage agreement regulating the usage of the tools and infrastructures.

3. Members of the Hosting Consortium shall conclude a written consortium agreement which sets out their internal arrangements for implementing the hosting and usage Agreement.

4. A Cross-border SOC shall 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 shall be responsible for compliance with the requirements of the hosting and usage agreement and of this Regulation.

Article 6

Cooperation and information sharing within and between cross-border SOCs

1. Members of a Hosting Consortium shall 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:

(a) aims to prevent, detect, respond to or recover from incidents or to mitigate their impact;

(b) 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.

2. The written consortium agreement referred to in Article 5(3) shall establish:

(a) a commitment to share a significant amount of data referred to in paragraph 1, and the conditions under which that information is to be exchanged;

(b) a governance framework incentivising the sharing of information by all participants;

(c) targets for contribution to the development of advanced artificial intelligence and data analytics tools.

3. To encourage exchange of information between Cross-border SOCs, Cross-border SOCs shall 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. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2) of this Regulation.

4. Cross-border SOCs shall conclude cooperation agreements with one another, specifying information sharing principles among the cross-border platforms.

Article 7

Cooperation and information sharing with Union entities

1. Where the Cross-border SOCs obtain information relating to a potential or ongoing large-scale cybersecurity incident, they shall provide relevant information to EU=CyCLONe, the CSIRTs network and the Commission, in view of their respective crisis management roles in accordance with Directive (EU) 2022/2555 without undue delay.

2. The Commission may, by means of implementing acts, determine the procedural arrangements for the information sharing provided for in paragraphs 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2) of this Regulation.

Article 8

Security

1. Member States participating in the European Cyber Shield shall ensure a high level of data security and physical security of the European Cyber Shield infrastructure, and shall ensure that the infrastructure shall be adequately managed and controlled in such a way as to protect it from threats and to ensure its security and that of the systems, including that of data exchanged through the infrastructure.

2. Member States participating in the European Cyber Shield shall 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.

3. The Commission may adopt implementing acts laying down technical requirements for Member States to comply with their obligation under paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2) of this Regulation. In doing so, the Commission, supported by the High Representative, shall take into account relevant defence-level security standards, in order to facilitate cooperation with military actors.

Chapter III

CYBER EMERGENCY MECHANISM

Article 9

Establishment of the Cyber Emergency Mechanism

1. A Cyber Emergency Mechanism is established to improve the Union's resilience to major cybersecurity threats and prepare for and mitigate, in a spirit of solidarity, the short-term impact of significant and large-scale cybersecurity incidents (the 'Mechanism').

2. Actions implementing the Cyber Emergency Mechanism shall be supported by funding from DEP and implemented in accordance with Regulation (EU) 2021/694 and in particular Specific Objective 3 thereof.

Article 10

Type of actions

1. The Mechanism shall support the following types of actions:

(a) preparedness actions, including the coordinated preparedness testing of entities operating in highly critical sectors across the Union;

(b) 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 established under Article 12;

(c) mutual assistance actions consisting of the provision of assistance from national authorities of one Member State to another Member State, in particular as provided for in Article 11(3), point (f), of Directive (EU) 2022/2555.

Article 11

Coordinated preparedness testing of entities

1. For the purpose of supporting the coordinated preparedness testing of entities referred to in Article 10(1), point (a), across the Union, the Commission, after consulting the NIS Cooperation Group and ENISA, shall identify the sectors, or sub-sectors, concerned, from the Sectors of High Criticality listed in Annex I to Directive (EU) 2022/2555 from which entities may be subject to the coordinated preparedness testing, taking into account existing and planned coordinated risk assessments and resilience testing at Union level.

2. The NIS Cooperation Group in cooperation with the Commission, ENISA, and the High Representative, shall develop common risk scenarios and methodologies for the coordinated testing exercises.

Article 12

Establishment of the EU Cybersecurity Reserve

1. An EU Cybersecurity Reserve shall be established, in order to assist users referred to in paragraph 3, in responding or providing support for responding to significant or large-scale cybersecurity incidents, and immediate recovery from such incidents.

2. The EU Cybersecurity Reserve shall consist of incident response services from trusted providers selected in accordance with the criteria laid down in Article 16. The Reserve shall include pre-committed services. The services shall be deployable in all Member States.

3. Users of the services from the EU Cybersecurity Reserve shall include:

(a) Member States' cyber crisis management authorities and CSIRTs as referred to in Article 9 (1) and (2) and Article 10 of Directive (EU) 2022/2555, respectively;

(b) Union institutions, bodies and agencies.

4. Users referred to in paragraph 3, point (a), shall use the services from the EU Cybersecurity Reserve in order to respond or support response to and immediate recovery from significant or large-scale incidents affecting entities operating in critical or highly critical sectors.

5. The Commission shall have overall responsibility for the implementation of the EU Cybersecurity Reserve. The Commission shall determine the priorities and evolution of the EU Cybersecurity Reserve, in line with the requirements of the users referred to in paragraph 3, and shall supervise its implementation, and ensure complementarity, consistency, synergies and

links with other support actions under this Regulation as well as other Union actions and programmes.

6. 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.

7. In order 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 shall prepare a similar mapping, after consulting the Commission, to identify the needs of third countries eligible for support from the EU Cybersecurity Reserve pursuant to Article 17. The Commission, where relevant, shall consult the High Representative.

8. The Commission may, by means of implementing acts, specify the types and the number of response services required for the EU Cybersecurity Reserve. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2).

Article 13

Requests for support from the EU Cybersecurity Reserve

1. The users referred to in Article 12(3) may request services from the EU Cybersecurity Reserve to support response to and immediate recovery from significant or large-scale cybersecurity incidents.

2. To receive support from the EU Cybersecurity Reserve, the users referred to in Article 12(3) shall 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.

3. Requests for support from users referred to in Article 12(3), point (a), of this Regulation shall be transmitted to the Commission and ENISA via the Single Point of Contact designated or established by the Member State in accordance with Article 8(3) of Directive (EU) 2022/2555.

4. Member States shall inform the CSIRTs network, and where appropriate EU-CyCLONe, about their requests for incident response and immediate recovery support pursuant to this Article.

5. Requests for incident response and immediate recovery support shall include:

(a) 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;

(b) information about measures taken to mitigate the incident for which the support is requested, as referred to in paragraph 2;

(c) 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.

6. ENISA, in cooperation with the Commission and the NIS Cooperation Group, shall develop a template to facilitate the submission of requests for support from the EU Cybersecurity Reserve.

7. The Commission may, by means of implementing acts, specify further the detailed arrangements for allocating the EU Cybersecurity Reserve support services. Those

implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2).

Article 14

Implementation of the support from the EU Cybersecurity Reserve

1. Requests for support from the EU Cybersecurity Reserve, shall be assessed by the Commission, with the support of ENISA or as defined in contribution agreements under Article 12(6), and a response shall be transmitted to the users referred to in Article 12(3) without delay.

2. To prioritise requests, in the case of multiple concurrent requests, the following criteria shall be taken into account, where relevant:

(a) the severity of the cybersecurity incident;

(b) the type of entity affected, with higher priority given to incidents affecting essential entities as defined in Article 3(1) of Directive (EU) 2022/2555;

(c) the potential impact on the affected Member State(s) or users;

(d) the potential cross-border nature of the incident and the risk of spill over to other Member States or users;

(e) the measures taken by the user to assist the response, and immediate recovery efforts, as referred in Article 13(2) and Article 13(5), point (b).

3. The EU Cybersecurity Reserve services shall 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 shall include liability conditions.

4. The agreements referred to in paragraph 3 may be based on templates prepared by ENISA, after consulting Member States.

5. The Commission and ENISA shall 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.

6. Within one month from the end of the support action, the users shall provide 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 as set out in Article 17, such report shall be shared with the High Representative.

7. The Commission shall report to the NIS Cooperation Group about the use and the results of the support, on a regular basis.

Article 15

Coordination with crisis management mechanisms

1. In cases where significant or large-scale cybersecurity incidents originate from or result in disasters as defined in Decision 1313/2013/EU[19], the support under this Regulation for

[19] Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism (OJ L 347, 20.12.2013, p. 924).

responding to such incidents shall complementactions under and without prejudice to Decision 1313/2013/EU.

2. 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 shall be handled in accordance with relevant protocols and procedures under the IPCR.

3. 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.

4. 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.

Article 16

Trusted providers

1. In procurement procedures for the purpose of establishing the EU Cybersecurity Reserve, the contracting authority shall act in accordance with the principles laid down in the Regulation (EU, Euratom) 2018/1046 and in accordance with the following principles:

(a) 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;

(b) ensure the protection of the essential security interests of the Union and its Member States.

(c) 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.

2. When procuring services for the EU Cybersecurity Reserve, the contracting authority shall include in the procurement documents the following selection criteria:

(a) the provider shall demonstrate 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;

(b) the provider, its subsidiaries and subcontractors shall 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;

(c) the provider shall provide 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;

(d) the provider shall have appropriate security clearance, at least for personnel intended for service deployment;

(e) the provider shall have the relevant level of security for its IT systems;

(f) the provider shall be equipped with the hardware and software technical equipment necessary to support the requested service;

(g) the provider shall be able to demonstrate that it has experience in delivering similar services to relevant national authorities or entities operating in critical or highly critical sectors;

(h) the provider shall be able to provide the service within a short timeframe in the Member State(s) where it can deliver the service;

(i) the provider shall be able to provide the service in the local language of the Member State(s) where it can deliver the service;

(j) once an EU certification scheme for managed security service Regulation (EU) 2019/881 is in place, the provider shall be certified in accordance with that scheme.

Article 17

Support to third countries

1. Third countries may request support from the EU Cybersecurity Reserve where Association Agreements concluded regarding their participation in DEP provide for this.

2. Support from the EU Cybersecurity Reserve shall be in accordance with this Regulation, and shall comply with any specific conditions laid down in the Association Agreements referred to in paragraph 1.

3. Users from associated third countries eligible to receive services from the EU Cybersecurity Reserve shall include competent authorities such as CSIRTs and cyber crisis management authorities.

4. Each third country eligible for support from the EU Cybersecurity Reserve shall designate an authority to act as a single point of contact for the purpose of this Regulation.

5. Prior to receiving any support from the EU Cybersecurity Reserve, third countries shall 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. Where provisions of Articles 13 and 14 of this Regulation refer to Member States, they shall apply to third countries as set out in paragraph 1.

6. The Commission shall coordinate with the High Representative about the requests received and the implementation of the support granted to third countries from the EU Cybersecurity Reserve.

Chapter IV

CYBERSECURITY INCIDENT REVIEW MECHANISM

Article 18

Cybersecurity Incident Review Mechanism

1. At the request of the Commission, the EU-CyCLONe or the CSIRTs network, ENISA shall 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 shall deliver an incident review report to the CSIRTs network, the EU-CyCLONe and the Commission to support them in carrying out their tasks, in particular in view of those set out in Articles 15 and 16 of Directive (EU) 2022/2555. Where relevant, the Commission shall share the report with the High Representative.

2. To prepare the incident review report referred to in paragraph 1, ENISA shall 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 shall 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.

3. The report shall cover a review and analysis of the specific significant or large-scale cybersecurity incident, including the main causes, vulnerabilities and lessons learned. It shall protect confidential information, in accordance with Union or national law concerning the protection of sensitive or classified information.

4. Where appropriate, the report shall draw recommendations to improve the Union's cyber posture.

5. Where possible, a version of the report shall be made available publicly. This version shall only include public information.

Chapter V

FINAL PROVISIONS

Article 19

Amendments to Regulation (EU) 2021/694

Regulation (EU) 2021/694 is amended as follows:

(1) Article 6 is amended as follows:

(a) paragraph 1 is amended as follows:

(1) the following point (aa) is inserted:

'(aa) support 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';

(2) the following point (g) is added:

'(g) establish and operate 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';

(a) Paragraph 2 is replaced by the following:

'2. The actions under Specific Objective 3 shall 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[20] with the exception of actions implementing the EU Cybersecurity Reserve, which shall be implemented by the Commission and ENISA.**';**

(2) Article 9 is amended as follows:

(a) in paragraph 2, points (b), (c) and (d) are replaced by the following:

'(b), EUR 1 776 956 000 for Specific Objective 2 – Artificial Intelligence;

(c), EUR 1 629 566 000 for Specific Objective 3 – Cybersecurity and Trust;

(d), EUR 482 347 000 for Specific Objective 4 – Advanced Digital Skills';

(b) the following paragraph 8 is added:

'8. By derogation to Article 12(4) of Regulation (EU, Euratom) 2018/1046, unused commitment and payment appropriations for actions pursuing the objectives set out in Article 6(1), point (g) of this Regulation, shall be automatically carried over and may be committed and paid up to 31 December of the following financial year.';

(3) In Article 14, paragraph 2 is replaced by the following:

[20] Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, (OJ L 202, 8.6.2021, p. 1-31).

"2. The Programme may provide funding in any of the forms laid down in the Financial Regulation, including in particular through procurement as a primary form, or grants and prizes.

Where the achievement of the objective of an action requires the procurement of innovative goods and services, grants may be awarded only to beneficiaries that are contracting authorities or contracting entities as defined in Directives 2014/24/EU [27] and 2014/25/EU [28] of the European Parliament and of the Council.

Where the supply of innovative goods or services that are not yet available on a large-scale commercial basis is necessary to achieve the objectives of an action, the contracting authority or the contracting entity may authorise the award of multiple contracts within the same procurement procedure.

For duly justified reasons of public security, the contracting authority or the contracting entity may require that the place of performance of the contract be situated within the territory of the Union.

When implementing procurement procedures for the EU Cybersecurity Reserve established by Article 12 of Regulation (EU) 2023/XX, the Commission and ENISA may act as a central purchasing body to procure on behalf of or in the name of third countries associated to the Programme in line with Article 10. The Commission and ENISA may also act as wholesaler, by buying, stocking and reselling or donating supplies and services, including rentals, to those third countries. By derogation from Article 169(3) of Regulation (EU). XXX/XXXX [FR Recast], the request from a single third country is sufficient to mandate the Commission or ENISA to act.

When implementing procurement procedures for the EU Cybersecurity Reserve established by Article 12 of Regulation (EU) 2023/XX, the Commission and ENISA may act as a central purchasing body to procure on behalf of or in the name of Union institutions, bodies and agencies. The Commission and ENISA may also act as wholesaler, by buying, stocking and reselling or donating supplies and services, including rentals, to Union institutions, bodies and agencies. By derogation from Article 169(3) of Regulation (EU) XXX/XXXX [FR Recast], the request from a single Union institution, body or agency is sufficient to mandate the Commission or ENISA to act.

The Programme may also provide financing in the form of financial instruments within blending operations."

(4) The following article 16a is added:

In the case of actions implementing the European Cyber Shield established by Article 3 of Regulation (EU) 2023/XX, the applicable rules shall be those set out in Articles 4 and 5 of Regulation (EU) 2023/XX. In the case of conflict between the provisions of this Regulation and Articles 4 and 5 of Regulation (EU) 2023/XX, the latter shall prevail and apply to those specific actions.

(5) Article 19 is replaced by the following:

'Grants under the Programme shall be awarded and managed in accordance with Title VIII of the Financial Regulation and may cover up to 100 % of the eligible costs, without prejudice to the co-financing principle as laid down in Article 190 of the Financial Regulation. Such grants shall be awarded and managed as specified for each specific objective.

Support in the form of grants may be awarded directly by the ECCC without a call for proposals to the National SOCs referred to in Article 4 of Regulation XXXX and the Hosting Consortium referred to in Article 5 of Regulation XXXX, in accordance with Article 195(1), point (d) of the Financial Regulation.

Support in the form of grants for the Cyber Emergency Mechanism as set out in Article 10 of Regulation XXXX may be awarded directly by the ECCC to Member States without a call for proposals, in accordance with Article 195(1), point (d) of the Financial Regulation.

For actions specified in Article 10(1), point (c) of Regulation 202X/XXXX, the ECCC shall inform the Commission and ENISA about Member States' requests for direct grants without a call for proposals.

For the support of mutual assistance for response to a significant or large-scale cybersecurity incident as defined in Article 10(c), of Regulation XXXX, and in accordance with Article 193(2), second subparagraph, point (a), of the Financial Regulation, in duly justified cases, the costs may be considered to be eligible even if they were incurred before the grant application was submitted.";

(6) Annexes I and II are amended in accordance with the Annex to this Regulation.

Article 20

Evaluation

By [four years after the date of application of this Regulation], the Commission shall submit a report on the evaluation and review of this Regulation to the European Parliament and to the Council.

Article 21

Committee procedure

1. The Commission shall be assisted by the Digital Europe Programme Coordination Committee established by Regulation (EU) 2021/694. That committee shall be a committee within the meaning of Regulation (EU) 182/2011.
2. Where reference is made to this paragraph, Article 5 of Regulation (EU) 182/2011 shall apply.

Article 22

Entry into force

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Strasbourg,

For the European Parliament	*For the Council*
The President	*The President*

LEGISLATIVE FINANCIAL STATEMENT

1. FRAMEWORK OF THE PROPOSAL/INITIATIVE

1.1. Title of the proposal/initiative

1.2. Policy area(s) concerned

1.3. The proposal/initiative relates to:

1.4. Objective(s)

1.4.1. General objective(s)

1.4.2. Specific objective(s)

1.4.3. Expected result(s) and impact

1.4.4. Indicators of performance

1.5. Grounds for the proposal/initiative

1.5.1. Requirement(s) to be met in the short or long term including a detailed timeline for roll-out of the implementation of the initiative

1.5.2. Added value of Union involvement (it may result from different factors, e.g. coordination gains, legal certainty, greater effectiveness or complementarities). For the purposes of this point 'added value of Union involvement' is the value resulting

from Union intervention, which is additional to the value that would have been otherwise created by Member States alone.

1.5.3. Lessons learned from similar experiences in the past

1.5.4. Compatibility with the Multiannual Financial Framework and possible synergies with other appropriate instruments

1.5.5. Assessment of the different available financing options, including scope for redeployment

1.6. Duration and financial impact of the proposal/initiative

1.7. Method(s) of budget implementation planned

2. MANAGEMENT MEASURES

2.1. Monitoring and reporting rules

2.2. Management and control system(s)

2.2.1. Justification of the management mode(s), the funding implementation mechanism(s), the payment modalities and the control strategy proposed

2.2.2. Information concerning the risks identified and the internal control system(s) set up to mitigate them

2.2.3. Estimation and justification of the cost-effectiveness of the controls (ratio of "control costs ÷ value of the related funds managed"), and assessment of the expected levels of risk of error (at payment & at closure)

2.3. Measures to prevent fraud and irregularities

3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE

3.1. Heading(s) of the multiannual financial framework and expenditure budget line(s) affected

3.2. Estimated financial impact of the proposal on appropriations

3.2.1. Summary of estimated impact on operational appropriations

3.2.2. Estimated output funded with operational appropriations

3.2.3. Summary of estimated impact on administrative appropriations

3.2.3.1. Estimated requirements of human resources

3.2.4. Compatibility with the current multiannual financial framework

3.2.5. Third-party contributions

3.3. Estimated impact on revenue

1. FRAMEWORK OF THE PROPOSAL/INITIATIVE

1.1. Title of the proposal/initiative

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

1.2. Policy area(s) concerned

A Europe fit for the Digital Age European Strategic Investments Activity: Shaping Europe's digital future.

1.3. The proposal/initiative relates to:

☒ a new action

☐ a new action following a pilot project/preparatory action[33]

☐ the extension of an existing action

☐ a merger or redirection of one or more actions towards another/a new action

1.4. Objective(s)

1.4.1. General objective(s)

The Cyber Solidarity Act will strengthen solidarity at Union level to better detect, prepare and respond to cybersecurity threats and incidents. It aims: (a) to strengthen common EU detection and situational awareness of cyber threats and incidents; (b) to reinforce preparedness of critical entities across the EU and strenghten solidarity by developing common response capacities against significant or large-scale cybersecurity incidents, including by via making incident response support available for third countries. associated to DEP; (c) to 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.

1.4.2. Specific objective(s)

The Cyber Solidarity Act will achieve the set of objectives through:

(a) The deployment of a pan-European infrastructure of Security Operation Centres (European Cyber Shield) to build and enhance common detection and situational awareness capabilities.

(b) The creation of a Cybersecurity Emergency Mechanism to support Member States in preparing for, responding to and immediate recovery from significant and large-scale cybersecurity incidents. Support for incident response shall also

[33] As referred to in Article 58(2)(a) or (b) of the Financial Regulation.

be made available to European institutions, bodies, offices and agencies of the Union (EUIBAs).

These actions will be supported by funding from DEP, which this legislative instrument will amend in order to establish the above mentioned actions, provide for financial support for their development and clarify the conditions for benefitting from the financial support.

(c) the establishment of a European Cybersecurity Incident Mechanism to review and assess significant or large-scale incidents.

1.4.3. Expected result(s) and impact

Specify the effects which the proposal/initiative should have on the beneficiaries/groups targeted.

The proposal would bring significant benefits to the various stakeholders. The European Cyber Shield will improve cyber threat detection capabilities of the Member States. The Cyber Emergency Mechanism will complement Member States' actions through emergency support for preparedness, response and immediate recovery/ restoring the functioning of essential services.

These actions will strengthen the competitive position of industry and business in Europe across the digitised economy and supporting their digital transformation, by reinforcing the level of cybersecurity in the Digital Single Market. In particular, it aims at increasing the resilience of citizens, businesses and entities operating in critical or highly critical sectors against the growing cybersecurity threats, which can have devastating societal and economic impacts. It will do so by investing in tools that will support a faster detection and response to cybersecurity threats and incidents, and will assist Member States in better preparing to, as well as responding to significant and large-scale cybersecurity incidents. This should also support endowing Europe with stronger capacities in these areas, notably as regards the collection and analysis of data on cybersecurity threats and incidents.

1.4.4. Indicators of performance

Specify the indicators for monitoring progress and achievements.

In order to promote solidarity at the Union level, several indicators could be taken into account:

(1) The number of cybersecurity infrastructure, or tools, or both jointly procured

(2) The Number of actions supporting preparedness and response to cybersecurity incidents under the Cyber Emergency Mechanism.

1.5. Grounds for the proposal/initiative

1.5.1. Requirement(s) to be met in the short or long term including a detailed timeline for roll-out of the implementation of the initiative

The Regulation should be fully applicable shortly after its adoption, i.e. on the twentieth day following that of its publication in the Official Journal of the European Union.

1.5.2. Added value of Union involvement (it may result from different factors, e.g. coordination gains, legal certainty, greater effectiveness or complementarities). For the purposes of this point 'added value of Union involvement' is the value resulting

from Union intervention, which is additional to the value that would have been otherwise created by Member States alone.

The strong cross-border nature of cybersecurity threats in general and the growing number of risks and incidents, which have spill-over effects across borders, sectors, and products, mean that the objectives of the present intervention cannot effectively be achieved by Member States alone and require common action and solidarity at Union level. The experience of countering cyber-threats stemming from the war against Ukraine, together with the lessons learned from a cybersecurity exercise conducted under the French Presidency (EU CyCLES), showed that concrete mutual support mechanisms, notably cooperation with the private sector, should be developed to achieve solidarity at EU level. Against this background, the Council Conclusions of 23 May 2022 on the development of the European Union's cyber posture calls upon the Commission to present a proposal on a new Emergency Response Fund for Cybersecurity. Support and actions at Union level to better detect cybersecurity threats, and to increase preparedness and response capacities provide added value because it avoids duplication of efforts across the Union and Member States. It would lead to a better exploitation of existing assets and to greater coordination and exchange of information on lessons learned.

1.5.3. Lessons learned from similar experiences in the past

Regarding situational awareness and detection under the European Cyber Shield, a call for expression of interest to jointly procure tools and infrastructure to establish Cross-border SOCs, and a call for grants to enable capacity building of SOCs serving public and private organisations, were held under DEP cybersecurity work programme 2021-2022.

As regards preparedness and incident response, the Commission has set up a short-term programme to support Member States, through additional funding allocated to ENISA, in order to immediately reinforce preparedness and capacities to respond to major cyber incident. Services covered include preparedness actions, such as penetration testing of critical entities in order to identify vulnerabilities. It also strengthens possibilities to assist Member States in case of a major incident affecting critical entities. The implementation by ENISA of this short-term programme is under way and has already provided relevant valuable insights that have been taken into account in the preparation of this Regulation

1.5.4. Compatibility with the Multiannual Financial Framework and possible synergies with other appropriate instruments

The Cyber Solidarity Act will build upon actions currently supported by the Union and Member States to enhance situational awareness and cyber threat detection, and to respond to large-scale and cross border cybersecurity incidents. In addition, the instrument is consistent with other frameworks of crisis management, including the IPCR, the Common Security and Defence Policy, including Cyber Rapid Response Teams, and the assistance provided by one Member State to another Member State in the context of Article 42(7) of the Treaty on the European Union. The new proposal would also complement and support structures developed under other cybersecurity instruments such as the Directive (EU) 2022/2555 (NIS2 Directive) or Regulation 2019/881 (the Cybersecurity Act).

1.5.5. Assessment of the different available financing options, including scope for redeployment

The management of the action areas assigned to ENISA fits its existing mandate and general tasks. These action areas may require specific profiles or new assignments, but these can be absorbed by the existing resources of ENISA and resolved through reallocation or linking of various assignments. ENISA is currently implementing a short-term programme that was set up in 2022 by the Commission to immediately reinforce preparedness and capacities to respond to major cyber incident. Services covered include possibilities to assist Member States in case of a major incident affecting critical entities. The implementation by ENISA of this short-term programme is under way and has already provided relevant valuable insights that have been taken into account in the preparation of this Regulation Resources allocated for the short-term programme could also be used in the context of this Regulation.

1.6. Duration and financial impact of the proposal/initiative

☒ **limited duration**

– ☒ in effect from date of adoption of the proposal for a Regulation of the European Parliament and of the Council on strengthening solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents ('the Cyber Solidarity Act')

– ☒ Financial impact from 2023 to 2027 for commitment appropriations and from 2023 to 2031 for payment appropriations[34].

☐ **unlimited duration**

– Implementation with a start-up period from YYYY to YYYY,

– followed by full-scale operation.

1.7. Method(s) of budget implementation planned[35]

☒ **Direct management** by the Commission

– ☒ by its departments, including by its staff in the Union delegations;

– ☐ by the executive agencies

☐ **Shared management** with the Member States

☒ **Indirect management** by entrusting budget implementation tasks to:

– ☐ third countries or the bodies they have designated;

– ☐ international organisations and their agencies (to be specified);

– ☐ the EIB and the European Investment Fund;

– ☒ bodies referred to in Articles 70 and 71 of the Financial Regulation;

– ☐ public law bodies;

– ☐ bodies governed by private law with a public service mission to the extent that they are provided with adequate financial guarantees;

– ☐ bodies governed by the private law of a Member State that are entrusted with the implementation of a public-private partnership and that are provided with adequate financial guarantees;

– ☐ bodies or persons entrusted with the implementation of specific actions in the CFSP pursuant to Title V of the TEU, and identified in the relevant basic act.

– *If more than one management mode is indicated, please provide details in the 'Comments' section.*

Comments

The actions related to the European Cyber Shield will be implemented by the ECCC. Until the ECCC has the capacity to implement its own budget, the European Commission will implement the actions in direct management on behalf of the ECCC. The ECCC may select entities based on calls for expression of interest to participate in joint procurement of tools. The ECCC may award grants for the operation of these tools.

[34] The actions in the Act should be supported by the next Multiannual Financial Framework.

[35] Details of budget implementation methods and references to the Financial Regulation may be found on the BUDGpedia site: https://myintracomm.ec.europa.eu/corp/budget/financial-rules/budget-implementation/Pages/implementation-methods.aspx

Moreover, the ECCC may award grants for preparedness actions under the Cybersecurity Emergency Mechanism.

The Commission shall have overall responsibility for the implementation of the EU Cybersecurity Reserve. The Commission may entrust, in full or in part, by means of contribution agreements, the operation and administration of the EU Cybersecurity Reserve to ENISA. The assigned actions of this Regulation to ENISA are in line with its existing mandate. Those actions include : (i) Supporting the NIS Cooperation Group in developing the preparedness actions according to risk assessments; (ii) Supporting the Commission in establishing and supervising the implementation of the EU Cybersecurity Reserve, including receiving and processing the requests for support; (iii) Developping templates to facilitate the submission of requests for support and specific agreements to be concluded between the service provider and the user to which the support under the EU Cybersecurity Reserve is provided; (iv) reviewing and assessing threats, vulnerabilities and mitigation actions with respect to a specific significant or large-scale cybersecurity incidents and preparing reports thereof.

All these assignments are estimated to about 7 FTEs from the existing resources of ENISA, building already on expertise and preparatory work that it is currently done by ENISA within the pilot of the emergency support for preparedness and incident response.

2. MANAGEMENT MEASURES

2.1. Monitoring and reporting rules

Specify frequency and conditions.

The Commission will monitor the implementation, the application and the compliance with these new provisions with a view to assessing their effectiveness. The Commission shall submit a report on the evaluation and review of this Regulation to the European Parliament and to the Council by four years after the date of its application.

2.2. Management and control system(s)

2.2.1. Justification of the management mode(s), the funding implementation mechanism(s), the payment modalities and the control strategy proposed

The Regulation introduces a framework for implementing EU funding with a view to increasing cybersecurity resilience through actions enhancing the detection, response and recovery capabilities in case of significant and large-scale cybersecurity incidents. The units within DG CNECT in charge of the policy field will manage the implementation of the Directive.

In order to face the new tasks, it is necessary to appropriately resource the Commission's services. The enforcement of the new Regulation is estimated to require 6 FTEs (3 AD and 3 CA) to cover the following tasks:

- Determining preparedness actions according to risk assessments;
- Ensuring interoperability between Cross-border SOC platforms;
- Elaborating potential Implementing Acts (two for SOCs and two for the Cybersecurity Emergency Mechanism);
- Managing the Hosting and Usage Agreements for SOCs;
- Establishing and managing the EU Cybersecurity Reserve, directly or via a contribution agreement to ENISA. In case of contribution agreement to ENISA, elaborating and supervising the implementation of the contribution agreement for the tasks assigned to ENISA;
- Participating in the consultation groups convened by ENISA to review and assess significant and large-scale cybersecurity incidents and preparing the reports.

2.2.2. Information concerning the risks identified and the internal control system(s) set up to mitigate them

A risk identified for the European Cyber Shield is that Member States do not share a sufficient amount of relevant cyber threat information either within the Cross-border SOC platforms, or between Cross-border platforms and other relevant entities at EU level. In order to mitigate these risks, the allocation of funding will follow a call for expression of interest where Member States commit to sharing a certain amount of information with the EU level. This commitment will then be formalised in a hosting and usage agreement, which will give the ECCC the powers to conduct audits to ensure the jointly procured tools and infrastructure are being used in accordance with the

agreement. Commitments to a high level of information sharing within the Cross-border SOCs will be formalised in a consortium agreement.

A risk identified for the Cyber Emergency Mechanism is that users participating in the mechanism do not take sufficient measures to ensure preparedness in the face of cyber attacks. For that reason, to be able to receive support from the EU Cybersecurity Reserve, users are obliged to take such preparedness measures. When submitting the requests for support to the EU Cybersercurity Reserve, users need to explain what measures have been taken already to respond to the incident, which will be taken into account during assessment of the requests to the EU Cybersecurity Reserve.

2.2.3. Estimation and justification of the cost-effectiveness of the controls (ratio of "control costs ÷ value of the related funds managed"), and assessment of the expected levels of risk of error (at payment & at closure)

As the rules for participation in the Digital Europe programme applicable to the support under the Cyber Solidarity Act are similar to those that the Commission will use in its work programmes, and with a population of beneficiaries with a similar risk profile to those of programmes under direct management, it can be expected that the error margin will be similar to that foreseen by the Commission for the Digital Europe programme, i.e. to give reasonable assurance that the risk of error over the course of the multiannual expenditure period is, on an annual basis, within a range of 2-5 %, with the ultimate aim to achieve a residual error rate as close as possible to 2 % at the closure of the multi-annual programmes, once the financial impact of all audits, correction and recofvery measures have been taken into account.

2.3. Measures to prevent fraud and irregularities

Specify existing or envisaged prevention and protection measures, e.g. from the Anti-Fraud Strategy.

In the case of the European Cyber Shield, the ECCC will have the power of audit, on the basis of access to information and on-the-spot checks, of the jointly procured tools and infrastructures, in accordance with the hosting and usage agreement to be signed between the hosting consortium and the ECCC.

The existing fraud prevention measures applicable to the Union institutions, bodies and agencies will cover the additional appropriations necessary for this Regulation.

3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE

3.1. Heading(s) of the multiannual financial framework and expenditure budget line(s) affected

- Existing budget lines

In order of multiannual financial framework headings and budget lines.

Heading of multiannual financial framework	Budget line	Type of expenditure	Contribution			
	Number	Diff./Non-diff.[36]	from EFTA countries [37]	from candidate countries and potential candidates [38]	fromother third countries	other assigned revenue
1	02 04 01 10 - Digital Europe programme - Cybersecurity	Diff.	YES	YES	NO	NO
1	02 04 01 11 - Digital Europe programme - European Cybersecurity Industrial, Technology and Research Competence Centre	Diff	YES	YES	NO	NO
1	02 04 03 - Digital Europe programme - Artificial intelligence	Diff	YES	YES	NO	NO
1	02 04 04 - Digital Europe programme – Skills	Diff	YES	YES	NO	NO
1	02 01 30 - Support expenditure for the Digital Europe programme	Non Diff	YES	YES	NO	NO

[36] Diff. = Differentiated appropriations / Non-diff. = Non-differentiated appropriations.
[37] EFTA: European Free Trade Association.
[38] Candidate countries and, where applicable, potential candidate countries.

3.2. Estimated financial impact of the proposal on appropriations

3.2.1. Summary of estimated impact on operational appropriations

– ☐ The proposal/initiative does not require the use of operational appropriations

– ☒ The proposal/initiative requires the use of operational appropriations, as explained below:

EUR million (to three decimal places)

Heading of multiannual financial framework	Number	1 **Single Market, Innovation and Digital**

The proposal will not increase the total level of commitments under the Digital Europe Programme. Indeed, the contribution to this initiative is a redistribution of the commitments coming from SO2 and SO4 to reinforce the budget of SO3 and ECCC. Any increase of commitments under the Digital Europe Programme stemming from a revision of the MFF could be used for the purpose of this initiative.

DG CONNECT			Year **2025**	Year **2026**	Year **2027**	Year **2028+**	Enter as many years as necessary to show the duration of the impact (see point 1.6)			**TOTAL**
○ Operational appropriations										
Budget line[39] 02.040110 (redistribution from 02.0403 and 02.0404)	Commitments	(1a)	15,000	15,000	6,000	p.m.				**36,000**
	Payments	(2a)	15,000	15,000	6,000					**36,000**
Budget line 02.040111.02 (redistribution from 02.0403 and 02.0404)	Commitments	(1b)	13,000	23,000	28,000	p.m.				**64,000**
	Payments	(2b)	8,450	18,200	25,250	12,100				**64,000**
Appropriations of an administrative nature financed from the envelope of specific programmes[40]										
Budget line 02.0130		(3)	0,150	0,150	0,150	p.m.				0,450
	Commitments	=1a+1b +3	**28,150**	**38,150**	**34,150**	**p.m.**				**100,450**

39 According to the official budget nomenclature.

40 Technical and/or administrative assistance and expenditure in support of the implementation of EU programmes and/or actions (former 'BA' lines), indirect research, direct research.

TOTAL appropriations for DG CONNECT	Payments	=2a+2b +3	**23,600**	**33,350**	**31,400**	**12,100**				**100,450**

○ TOTAL operational appropriations	Commitments	(4)	28,000	38,000	34,000	p.m.				**100,000**
	Payments	(5)	23,450	33,200	31,250	12,100				**100,000**
○ TOTAL appropriations of an administrative nature financed from the envelope for specific programmes		(6)	0,150	0,150	0,150	p.m.				**0,450**
TOTAL appropriations under HEADING 1 of the multiannual financial framework	Commitments	=4+ 6	**28,150**	**38,150**	**34,150**	**p.m.**				**100,450**
	Payments	=5+ 6	**23,600**	**33,350**	**31,400**	**12,100**				**100,450**

If more than one operational heading is affected by the proposal / initiative, repeat the section above:

○ TOTAL operational appropriations (all operational headings)	Commitments	(4)	28,000	38,000	34,000	p.m.				**100,000**
	Payments	(5)	23,450	33,200	31,250	12,100				**100,000**
TOTAL appropriations of an administrative nature financed from the envelope for specific programmes (all operational headings)		(6)	0,150	0,150	0,150					**0,450**
TOTAL appropriations under HEADINGS 1 to 6 of the multiannual financial framework (Reference amount)	Commitments	=4+ 6	**28,150**	**38,150**	**34,150**	**p.m.**				**100,450**
	Payments	=5+ 6	**23,600**	**33,350**	**31,400**	**12,100**				**100,450**

Heading of multiannual financial framework	7	'Administrative expenditure'

This section should be filled in using the 'budget data of an administrative nature' to be firstly introduced in the Annex to the Legislative Financial Statement (Annex 5 to the Commission decision on the internal rules for the implementation of the Commission section of the general budget of the European Union), which is uploaded to DECIDE for interservice consultation purposes.

EUR million (to three decimal places)

		Year **2025**	Year **2026**	Year **2027**	Year **2028+**	Enter as many years as necessary to show the duration of the impact (see point 1.6)			**TOTAL**
DG: CONNECT									
○ Human resources		0,786	0,786	0,786	p.m.				**2,358**
○ Other administrative expenditure		0,035	0,035	0,035	p.m.				**0,105**
TOTAL DG CONNECT	Appropriations	**0,821**	**0,821**	**0,821**					**2,463**

TOTAL appropriations under HEADING 7 of the multiannual financial framework	(Total commitments = Total payments)	**0,821**	**0,821**	**0,821**					**2,463**

EUR million (to three decimal places)

		Year **2025**	Year **2026**	Year **2027**	Year **2028+**	Enter as many years as necessary to show the duration of the impact (see point 1.6)			**TOTAL**
TOTAL appropriations under HEADINGS 1 to 7 of the multiannual financial framework	Commitments	**28,971**	**38,971**	**34,971**	**p.m.**				**102,913**
	Payments	**24,421**	**34,171**	**32,221**	**12,100**				**102,913**

3.2.2. Estimated output funded with operational appropriations

Commitment appropriations in EUR million (to three decimal places)

Indicate objectives and outputs ⇩			Year **N**		Year **N+1**		Year **N+2**		Year **N+3**		Enter as many years as necessary to show the duration of the impact (see point 1.6)						**TOTAL**	
	OUTPUTS																	
	Type[41]	Average cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	Total No	Total cost
SPECIFIC OBJECTIVE No 1[42]…																		
- Output																		
- Output																		
- Output																		
Subtotal for specific objective No 1																		
SPECIFIC OBJECTIVE No 2 ...																		
- Output																		
Subtotal for specific objective No 2																		
TOTALS																		

41 Outputs are products and services to be supplied (e.g.: number of student exchanges financed, number of km of roads built, etc.).

42 As described in point 1.4.2. 'Specific objective(s)…'

3.2.3. Summary of estimated impact on administrative appropriations

– ☐ The proposal/initiative does not require the use of appropriations of an administrative nature

– ☒ The proposal/initiative requires the use of appropriations of an administrative nature, as explained below:

EUR million (to three decimal places)

	Year 2025	Year r 2026	Year 2027	Year N+3	Enter as many years as necessary to show the duration of the impact (see point 1.6)			**TOTAL**
HEADING 7 of the multiannual financial framework								
Human resources	0,786	0,786	0,786					**2,358**
Other administrative expenditure	0,035	0,035	0,035					**0,105**
Subtotal HEADING 7 of the multiannual financial framework	**0,821**	**0,821**	**0,821**					**2,463**

Outside HEADING 7[43] of the multiannual financial framework								
Human resources								
Other expenditure of an administrative nature	0,150	0,150	0,150					**0,450**
Subtotal outside HEADING 7 of the multiannual financial framework	**0,150**	**0,150**	**0,150**					**0,450**

TOTAL	**0,971**	**0,971**	**0,971**					**2,913**

The appropriations required for human resources and other expenditure of an administrative nature will be met by appropriations from the DG that are already assigned to management of the action and/or have been redeployed within the DG, together if necessary with any additional allocation which may be granted to the managing DG under the annual allocation procedure and in the light of budgetary constraints.

[43] Technical and/or administrative assistance and expenditure in support of the implementation of EU programmes and/or actions (former 'BA' lines), indirect research, direct research.

3.2.3.1. Estimated requirements of human resources

– ☐ The proposal/initiative does not require the use of human resources.

– ☒ The proposal/initiative requires the use of human resources, as explained below:

Estimate to be expressed in full time equivalent units

		Year **2025**	Year **2026**	Year 2027	Year **N+3**	Enter as many years as necessary to show the duration of the impact (see point 1.6)		
O Establishment plan posts (officials and temporary staff)								
20 01 02 01 (Headquarters and Commission's Representation Offices)		3	3	3				
20 01 02 03 (Delegations)								
01 01 01 01 (Indirect research)								
01 01 01 11 (Direct research)								
Other budget lines (specify)								
O External staff (in Full Time Equivalent unit: FTE)[44]								
20 02 01 (AC, END, INT from the 'global envelope')		3	3	3				
20 02 03 (AC, AL, END, INT and JPD in the delegations)								
XX 01 xx **yy zz** [45]	- at Headquarters							
	- in Delegations							
01 01 01 02 (AC, END, INT - Indirect research)								
01 01 01 12 (AC, END, INT - Direct research)								
Other budget lines (specify)								
TOTAL		**6**	**6**	**6**				

XX is the policy area or budget title concerned.

The human resources required will be met by staff from the DG who are already assigned to management of the action and/or have been redeployed within the DG, together if necessary with any additional allocation which may be granted to the managing DG under the annual allocation procedure and in the light of budgetary constraints.

Description of tasks to be carried out:

Officials and temporary staff	- determining preparedness actions according to risk assessments (art 11) - Elaborating potential Implementing Acts (two for SOCs and two for the Cybersecurity Emergency Mechanism) - Managing the Hosting and Usage Agreements for SOCs; - Establishing and managing the EU Cybersecurity Reserve, directly or via a contribution agreement to ENISA.
External staff	Under the supervision of an official, - determining preparedness actions according to risk assessments (art 11) - Elaborating potential Implementing Acts (two for SOCs and two for the Cybersecurity Emergency Mechanism) - Managing the Hosting and Usage Agreements for SOCs; - Establishing and managing the EU Cybersecurity Reserve, directly or via a contribution agreement to ENISA.

[44] AC= Contract Staff; AL = Local Staff; END= Seconded National Expert; INT = agency staff; JPD= Junior Professionals in Delegations.

[45] Sub-ceiling for external staff covered by operational appropriations (former 'BA' lines).

3.2.4. *Compatibility with the current multiannual financial framework*

The proposal/initiative:

– [X] can be fully financed through redeployment within the relevant heading of the Multiannual Financial Framework (MFF).

Explain what reprogramming is required, specifying the budget lines concerned and the corresponding amounts. Please provide an excel table in the case of major reprogramming.

	2023	2024	2025	2026	2027	total
SO1	16.232.897	20.528.765	17.406.899	16.223.464	10.022.366	80.414.391
SO2 initial	226.316.819	295.067.000	195.649.000	221.809.000	246.608.000	1.185.449.819
To CYBER initiative			18.000.000	28.000.000	19.000.000	65.000.000
NEW SO2	**226.316.819**	**295.067.000**	**177.649.000**	**193.809.000**	**227.608.000**	**1.120.449.819**
SO3 DB 24	24.361.553	35.596.172	3.638.000	3.638.000	11.175.000	78.408.725
Fom SO2-SO4			15.000.000	15.000.000	6.000.000	36.000.000
New SO3	**24.361.553**	**35.596.172**	**18.638.000**	**18.638.000**	**17.175.000**	**114.408.725**
ECCC initial	176.222.303	208.374.879	104.228.130	90.704.986	84.851.497	664.381.795
From SO2-SO4			13.000.000	23.000.000	28.000.000	64.000.000
New ECCC	**176.222.303**	**208.374.879**	**117.228.130**	**113.704.986**	**112.851.497**	**728.381.795**
SO4 initial	66.902.708	64.892.032	56.577.977	70.477.245	72.107.201	330.957.163
To CYBER initiative			10.000.000	10.000.000	15.000.000	35.000.000
NEW SO4	**66.902.708**	**64.892.032**	**46.577.977**	**60.477.245**	**57.107.201**	**295.957.163**

– [ ] requires use of the unallocated margin under the relevant heading of the MFF and/or use of the special instruments as defined in the MFF Regulation.

Explain what is required, specifying the headings and budget lines concerned, the corresponding amounts, and the instruments proposed to be used.

– [ ] requires a revision of the MFF.

Explain what is required, specifying the headings and budget lines concerned and the corresponding amounts.

3.2.5. *Third-party contributions*

The proposal/initiative:

– [X] does not provide for co-financing by third parties

– [ ] provides for the co-financing by third parties estimated below:

Appropriations in EUR million (to three decimal places)

	Year N[46]	Year N+1	Year N+2	Year N+3	Enter as many years as necessary to show the duration of the impact (see point 1.6)			Total
Specify the co-financing body								

[46] Year N is the year in which implementation of the proposal/initiative starts. Please replace "N" by the expected first year of implementation (for instance: 2021). The same for the following years.

TOTAL appropriations co-financed								

3.3. Estimated impact on revenue

– ☒ The proposal/initiative has no financial impact on revenue.

– ☐ The proposal/initiative has the following financial impact:

  – ☐ on own resources

  – ☐ on other revenue

  – please indicate, if the revenue is assigned to expenditure lines ☐

EUR million (to three decimal places)

Budget revenue line:	Appropriations available for the current financial year	Impact of the proposal/initiative[47]						
		Year **N**	Year **N+1**	Year **N+2**	Year **N+3**	Enter as many years as necessary to show the duration of the impact (see point 1.6)		
Article …….								

For assigned revenue, specify the budget expenditure line(s) affected.

[…]

Other remarks (e.g. method/formula used for calculating the impact on revenue or any other information).

[…]

[47] As regards traditional own resources (customs duties, sugar levies), the amounts indicated must be net amounts, i.e. gross amounts after deduction of 20 % for collection costs.

EUROPEAN
COMMISSION

Strasbourg, 18.4.2023
COM(2023) 209 final

ANNEX

ANNEXES

to the

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

ANNEX

Regulation (EU) 2021/694 is amended as follows:

(1)In Annex I, the section/ chapter 'Specific Objective 3 – Cybersecurity and Trust' is replaced by the following:

'Specific Objective 3 – Cybersecurity and Trust

The Programme shall stimulate the reinforcement, building and acquisition of essential capacities to secure the Union's digital economy, society and democracy by reinforcing the Union cybersecurity industrial potential and competitiveness, as well as by improving capabilities of both the private and public sectors to protect citizens and businesses from cyber threats, including by supporting the implementation of Directive (EU) 2016/1148.

Initial and, where appropriate, subsequent actions under this objective shall include:

1. Co-investment with Member States in advanced cybersecurity equipment, infrastructures and knowhow that are essential to protect critical infrastructures and the Digital Single Market at large. Such co-investment could include investments in quantum facilities and data resources for cybersecurity, situational awareness in cyberspace ***including National SOCs and Cross-border SOCs forming the European Cyber Shield***, as well as other tools to be made available to public and private sector across Europe.

2. Scaling up existing technological capacities and networking the competence centres in Member States and making sure that those capacities respond to public sector and industry needs, including through products and services that reinforce cybersecurity and trust within the Digital Single Market.

3. Ensuring wide deployment of effective state-of-the-art cybersecurity and trust solutions across the Member States. Such deployment includes strengthening the security and safety of products, from their design to their commercialisation.

4. Support closing the cybersecurity skills gap by, for example, aligning cybersecurity skills programmes, adapting them to specific sectorial needs and facilitating access to targeted specialised training.

5. ***Promoting solidarity among Member States in preparing for and responding to significant cybersecurity incidents through deployment of cybersecurity services across borders,***

including support for mutual assistance between public authorities and the establishment of a reserve of trusted cybersecurity providers at Union level.';

(2) In Annex II the section/chapter 'Specific Objective 3 – Cybersecurity and Trust' is replaced by the following:

'Specific Objective 3 – Cybersecurity and Trust

3.1. The number of cybersecurity infrastructure, or tools, or both jointly procured[1]

3.2. The number of users and user communities getting access to European cybersecurity facilities

3.3 The number of actions supporting preparedness and response to cybersecurity incidents under the Cyber Emergency Mechanism'

ANNEX […]

Com 209 (2023)

Information Note

1. Proposal

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

2. Date of Commission document
18/04/2023

3. Number of Commission document
COM (2023) 209

4. Number of Council document:
2023/0109

5. Dealt with in Brussels by
Telecommunications Council / Horizontal Working Party on Cyber Issues

6. Department with primary responsibility
Department of the Environment, Climate and Communications

7. Other Departments involved
Department of Foreign Affairs

8. Background to, Short summary and aim of the proposal
Background to Proposal
The Council Conclusions of October 2021 highlighted the need to address these gaps, by calling for the Commission to present a proposal on a new Emergency Response Fund for Cybersecurity. The EU Cybersecurity Strategy adopted in December 2020 included provision for an European Cyber Shield, to develop cyber information sharing capabilities in the European Union by establishing Security Operations Centres (SOCs) on a national and cross-border basis to enhance detection and response capabilities.

Short Summary
The Commission's proposal – also referred to as the Cyber Solidarity Act – seeks to strengthen solidarity at Union level in order to better detect, prepare and respond to cybersecurity threats and incidents through the following specific objectives:

- *to strengthen common EU detection and situational awareness of cyber threats and incidents, and thus contribute to European technological sovereignty in the area of cybersecurity;*
- *to reinforce preparedness of critical entities across the EU and strengthen solidarity by developing common response capacities against significant or large-scale cybersecurity incidents, including by making incident response support available for third countries. associated to the Digital Europe Programme*
- *to 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

The proposal would draw on funding from the Digital Europe Programme to establish the European Cyber Shield and Cyber Emergency Mechanism. The Cyber Emergency Mechanism will ensure that preparedness and response to cybersecurity incidents are improved by testing entities in crucial sectors such as finance, energy and healthcare for potential weaknesses that could make them vulnerable to cyber threats, creating an EU Cybersecurity Reserve made up of incident response services from private service providers that can be deployed at the request of Member States or Union Institutions, bodies and agencies, to help them address significant or large-scale cybersecurity incidents, as well as
a mechanism to support a Member State that offers mutual assistance to another Member State affected by a cybersecurity incident.

Aim of Proposal

The Proposal has three aims:

- *The deployment of a pan-European infrastructure of SOCs (European Cyber Shield) to build and enhance common detection and situational awareness capabilities.*
- *The creation of a Cyber Emergency Mechanism to support Member States in preparing for, responding to and immediate recovery from significant and large-scale cybersecurity incidents. Support for incident response shall also be made available to European institutions, bodies, offices and agencies of the Union (EUIBAs).*
- *The establishment of a European Cybersecurity Incident Review Mechanism to review and assess specific significant or large-scale incidents.*

9. Legal basis of the proposal

The legal basis for this proposal is Article 173(3) and Article 322(1), point (a) of the Treaty on the Functioning of the European Union (TFEU). Article 173 TFEU provides that the Union and the Member States shall ensure that the conditions necessary for the competitiveness of the Union's industry exists. This Regulation aims at strengthening the competitive position of industry and service sectors in Europe across the digitised economy and supporting their digital transformation, by reinforcing the level of cybersecurity in the Digital Single Market. In particular, it aims at increasing the resilience of citizens, businesses and entities operating in critical and highly critical sectors against the growing cybersecurity threats, which can have devastating societal and economic impacts.

The proposal is based also on Article 322(1), point (a) TFEU because it contains specific carry-over rules derogating from the principle of annuality set out in Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council (the 'Financial Regulation')For the purpose of sound financial management and considering the unpredictable, exceptional and specific nature of the cybersecurity landscape and cyberthreats, the Cybersecurity Emergency Mechanism should benefit from a certain degree of flexibility in relation to budgetary management, and in particular by allowing unused commitment and payment appropriations for actions pursuing the objectives set out in the Regulation to be automatically carried over to the following financial year. As this new rule raises issues with the Financial Regulation, this matter could be addressed in the context of the current negotiations of the Financial Regulation recast.

10. Voting Method

QMV

11. Role of the EP
Co-decision

12. Category of proposal
Some significance

13. Implications for Ireland & Ireland's Initial View'
Ireland welcomes the proposal in principle and has already engaged with the European Commission with regard to the Cyber Shield Initiative and related funding calls under the Digital Europe Programme. Further analysis and consultation are required on the proposed reallocation of funding to the Strategic Objective 'Cybersecurity' under the DEP.

14. Impact on the public
The proposal has the potential to improve capacity in the Union to detect, prevent, respond to and recover from major cybersecurity incidents, which impact on national security, essential services, and livelihoods. The proposal could enhance the cyber resilience of critical infrastructure and essential service, with benefits for the public.

15. Have any consultations with Stakeholders taken place or are there any plans to do so?
Yes. The actions of this Regulation will be supported by DEP, which was subject to wide consultation. In addition, they will build on first steps that have been prepared in close cooperation with the main stakeholders. As regards SOCs, the Commission has developed a concept paper on the development of cross-border SOCs platforms and a Call for Expression of Interest in close cooperation with Member States in the framework of the European Cybersecurity Competence Centre (ECCC). In this context, a survey of national SOCs capacities was conducted and common approaches and technical requirements have been discussed within the technical working group of the ECCC that gathers representatives of EN 7 EN Member States. In addition, exchanges took place with industry, notably through the expert group on SOCs created by ENISA and the European Cyber Security Organisation (ECSO).
Secondly, as regards preparedness and incident response, the Commission has set up a short-term programme to support Member States, through additional funding allocated to ENISA from DEP, to immediately reinforce preparedness and capacities to respond to major cyber incidents. Member States' and industry's feedback gathered during the implementation of this short-term programme is already providing valuable insights that have fed into the preparation of the proposed Regulation to address identified shortcomings. This was a first step in line with the Council conclusions on the Cyber posture requesting the Commission to come forward with a proposal for a new Emergency Response Fund for Cybersecurity.
In addition, a workshop with Member States experts on the Cyber Emergency Mechanism was held on 16 February 2023, on the basis of a discussion paper. All Member States participated in this workshop and eleven Member States provided further contributions in writing.
Due to the urgent nature of the proposal, no impact assessment was carried out.

16. Are there any subsidiarity issues for Ireland?
No. The cross-border nature of cyber security threats leads to a requirement for the Government to engage with partners in the EU Member States, institutions, bodies and agencies to enhance our shared capacity to detect, prevent, respond to and recover from cyber security incidents. Ireland plays an active role in the cooperative structures established in the EU, and with like-minded third countries.

17. Anticipated negotiating period
Not known at this time.

18. Proposed implementation date
Not known at this time.

19. Consequences for national legislation
Brief description of implementation measures

20. Method of Transposition into Irish law
Regulation becomes directly applicable upon signature – no transposition required

21. Anticipated Transposition date
Not known at this time.

22. Consequences for the EU budget in Euros annually
The actions of this Regulation will be supported by funding under Strategic Objective 'Cybersecurity' of the Digital Europe Programme. The proposal includes provision to reallocate €100 million from other Strategic Objectives of DEP, bringing the total amount available for Cybersecurity actions under the DEP to €842.8 million over the period 2021-2027.

23. Contact name, telephone number and e-mail address of official in Department with primary responsibility
Peter Hogan, 0879739846, Peter.Hogan@decc.gov.ie

16 May 2023