Council of the European Union
General Secretariat



**Brussels, 02 October 2023**

**WK 12371/2023 INIT**

**LIMITE**

**CYBER**

*This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.*

**WORKING DOCUMENT**

| | |
|---|---|
| From: | Presidency |
| To: | Horizontal Working Party on cyber issues (attachés) |
| Subject: | 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 - Presidency compromise |

Following the discussion at the meeting of the Horizontal Working Party on Cyber Issues on 25 September 2023, as well as subsequent delegations' written comments, delegations will find in the Annex a Presidency compromise on the above legislative proposal.

The changes are indicated as compared to the Commission proposal and marked in bold or bold/ strikethrough.

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

---

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

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 reinforcing the level of cybersecurity in the Digital Single Market. As recommended in three different proposals of the Conference on the Future of Europe[1] , 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[2], Commission

---

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

2 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).

Recommendation (EU) 2017/1584[1], Directive 2013/40/EU of the European Parliament and of the Council[2] and Regulation (EU) 2019/881 of the European Parliament and of the Council[3]. 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[4].

(6) The Joint Communication on the EU Policy on Cyber Defence[5] 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 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'

---

1 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).

2 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).

3 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).

4 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)

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

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[1] 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

---

[1] 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).

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 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[1].

(13) **Participation in the European ~~Cyber Shield~~ Cybersecurity Alert System should be voluntary for Member States.** Each Member State **that decides to join the European ~~Cyber Shield~~ Cybersecurity Alert System** should designate a **National SOC hub.** ~~public body at national level tasked with coordinating cyber threat detection activities in that~~

[1] 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).

~~Member State.~~ These National SOC~~s~~ **hubs** should **have** ~~act~~ as **functionalities the capacity to act as** a reference point and gateway at national level for participation in the European ~~Cyber Shield~~ **Cybersecurity Alert System** and should **be capable of detecting, aggregating and analysing data relevant to cyber threats and incidents, by using in particular state-of-the-art technologies. They should also** ensure that cyber threat information from public and private entities is shared and collected at national level in an effective and streamlined manner. **Member States should be able to decide to designate an existing entity such as a CSIRT to conduct the functions of National SOC hub, or establish a new one. Member States should also be able to decide to designate different entities to carry out the different functionalities of the National SOC hub.**

(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.

(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, **correlating,** sharing and exchanging data, the European ~~Cyber Shield~~ **Cybersecurity Alert System** 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~~ **Cybersecurity Alert System** with the pan-European High Performance Computing infrastructure established by Council Regulation (EU) 2021/1173[1].

(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

---

[1] 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).

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 of Article 42(7) of TEU, the PESCO Cyber Rapid Response Teams[1] 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.

---

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

(26) This instrument is without prejudice to procedures and frameworks to coordinate crisis response at Union level, in particular the UCPM[1], IPCR[2], 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.

---

1 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).

2 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.

(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 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[1]. 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

---

[1] 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

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 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~~ **Cybersecurity Alert System**') 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, **mitigating the impact** and **inititating** ~~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 **and enhance Member States cyber resilience** through **the** 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 **enhanced** ~~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 **upon request and in coordination with Member States.**

3. This Regulation is without prejudice to the Member States' ~~primary~~ responsibility for **safeguarding** national security~~, public security,~~ **and their power to safeguard other essential State functions, including ensuring the territorial integrity of the State and maintaining law and order.** ~~and the prevention, investigation, detection and prosecution of criminal offences.~~

*Article 2*

**Definitions**

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

**(-1) 'National Security Operations Centre Hub' ("National SOC hub") means an entity designated by and under the authority of a Member State, which has the following functionalities:**

**(a) it has 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 cyber threats and incidents and contributing to a Cross-border SOC platform;**

**(b) it is capable of detecting, aggregating, and analysing data relevant to cyber threats and incidents by using in particular state of the art technologies;**

**(1) 'Cross-border Security Operations Centre Platform' ("Cross-border SOC Platform")** means a multi-country platform, **established by a written consortium agreeement** that brings together in a coordinated network structure **N**~~n~~ational SOCs **Hubs** from at least three Member States ~~who form a Hosting Consortium~~, and that is designed to **monitor, detect and analyse** ~~prevent~~ cyber threats ~~and~~ **to prevent** incidents and to support the production of **cyber threat** ~~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[1];~~

(3) **'Hosting Consortium'** means a consortium composed of participating **Member S**~~s~~tates, ~~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 **Platform**;

(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;

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

(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;

---

1 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).

~~(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;~~

~~(11)~~ **(8a)** **'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.

**(8b) 'CSIRT' means a CSIRT designated or established pursuant to Article 10 of Directive (EU) 2022/2555 .**

# Chapter II

## *THE EUROPEAN ~~CYBER SHIELD~~ CYBERSECURITY ALERT SYSTEM*

*Article 3*

### Establishment of the European ~~Cyber Shield~~ Cybersecurity Alert System

1. An interconnected pan-European infrastructure **that consist** of **National SOC hubs and Cross-border SOC platforms joining on a voluntary basis** ~~Security Operations Centres ('European Cyber Shield~~ **the Cybersecurity Alert System**[2]~~)~~ shall be established to **support the** develop**ment of** 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~~ **Cybersecurity Alert System** shall:

(a) pool and share data on cyber threats and incidents from various sources through cross-border SOC~~s~~ **platforms**;

(b) produce high-quality, actionable information and cyber threat intelligence, through the use of state-of-the art tools **and advanced technologies, such as** ~~, notably~~ Artificial Intelligence and data analytics ~~technologies~~;

(c) contribute to better protection and response to cyber threats **and incidents by relevant entities such as competent authorities designated or established pursuant to Article 8 of Directive (EU) 2022/2555, CSIRTs and the CSIRTs network**;

(d) contribute to **enhanced** ~~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 **of** advanced **tools and technologies, such as** 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.

**3. Actions implementing the European ~~Cyber Shield~~ Cybersecurity Alert System 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.**

*Article 4*

**National Security Operations Centre~~s~~ <u>Hubs</u>**

1. ~~In order~~ **Where a Member State decides** to participate in the European ~~Cyber Shield~~ **Cybersecurity Alert System**, ~~each Member State~~ **it** shall designate at least one National SOC **Hub**. ~~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, **Member States intending to participate in the European ~~Cyber Shield~~ Cybersecurity Alert System** ~~National SOCs~~ shall be selected by the European Cybersecurity Competence Centre ('ECCC') to **take part** ~~participate~~ in a joint procurement of tools and infrastructures with the ECCC**, in order to set up National SOC hubs or enhance capabilities of an existing one**. The ECCC may award grants to the selected **Member States** ~~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 **Member State** ~~National SOC~~ shall conclude a hosting and usage agreement regulating the usage of the tools and infrastructures.

3. A **Member State**~~National SOC~~ selected pursuant to paragraph 2 shall commit to apply **for their National SOC hubs** to participate in a Cross-border SOC **Platform** 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 **Member State's** National SOC **hub** is not a participant in a Cross-border SOC **Platform** by that time, **the Member State** ~~it~~ shall not be eligible for additional Union support under this Regulation.

*Article 5*

**Cross-border Security Operations Centres~~ Platforms~~**

1. A Hosting Consortium consisting of at least three Member States, ~~represented by National SOCs~~, committed to **ensuring that their National SOC hubs work** ~~working~~ together to coordinate their cyber-detection and threat monitoring activities shall be eligible to participate in actions to establish a Cross-border SOC **Platform**.

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 **member of the Hosting Consortium** ~~National SOC~~ acting as **a coordinator** ~~coordinating SOC~~, or by the Hosting Consortium if it has legal personality. The **coordinator** ~~co-ordinating SOC~~ shall be responsible for compliance **of the Cross-border SOC Platform** 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 ~~Platforms~~**

1. Members of a Hosting Consortium shall **ensure that their National SOC hubs** exchange**, in accordance with the Consortium Agreement,** relevant information among themselves within the Cross-border SOC **Platform** 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 **among the members of the Consortium** ~~a significant amount of data~~ **information** 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 **referred to in paragraph 1** by all participants;

(c) targets for contribution to the development of advanced **tools and technologies, such as** artificial intelligence and data analytics ~~tools~~.

3. To encourage exchange of information between Cross-border SOC~~s~~ **Platforms**, Cross-border SOC~~s~~**Platforms** shall ensure a high level of interoperability between themselves. To facilitate the interoperability between the Cross-border SOC~~s~~**Platforms**, 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 SOC~~s~~ **Platforms** 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 SOC~~s~~**Platforms** 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~~ **Cybersecurity Alert System** shall ensure a high level of data security and physical security of the European ~~Cyber Shield~~ **Cybersecurity Alert System** 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~~ **Cybersecurity Alert System** shall ensure that the sharing of information within the European ~~Cyber Shield~~ **Cybersecurity Alert System** 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 **support** improve**ment of** the Union's resilience to ~~major~~ cyber~~security~~ 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~~

      **(i)** the coordinated preparedness testing of entities operating in highly critical sectors across the Union;

      **(ii) other preparedness actions for entities operating in critical and highly critical sectors;**

   (b) ~~response~~ actions~~,~~ supporting response to and **initiating** ~~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 **technical support** ~~assistance~~ from ~~national authorities~~ ~~of~~ one Member State to another Member State, **including** ~~in particular~~ as provided for in Article 11(3), point (f), of Directive (EU) 2022/2555.

**2. Member States may benefit from the actions referred to in paragraph 1 upon request.**

*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 **Member States may propose** entities to ~~may~~ be subject to the coordinated preparedness testing**.**~~,~~

**1.a. When identifying the sectors or sub-sectors under paragraph 1, the Commission shall take** ~~taking~~ into account existing and planned coordinated risk assessments and resilience testing at Union level**, and the results thereof**.

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**, upon request,** 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~~ **Reserve** 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.

   **(c) Users of associated third countries in accordance with Article 17(3).**

4. Users referred to in paragraph 3, point (a), shall use the services **granted upon their request** from the EU Cybersecurity Reserve in order to respond or support response to and **initiate** ~~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**, in cooperation with the NIS Cooperation Group and ENISA,** 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 **and their availability**, 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 **initiate** ~~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**, where appropriate,** 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 **initiate** ~~immediate~~ recovery support pursuant to this Article.

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

(a) appropriate information regarding the affected entity and potential impacts of the incident **on affected Member State(s) and users, including the risk of spill over,** 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) **where relevant, available** information about other forms of support available to the affected entity, including contractual arrangements in place for incident response and **initial** ~~immediate~~ recovery services, as well as insurance contracts potentially covering such type of incident.

**5a. The information provided in accordance with paragraph 5 of this Article shall be handled in accordance with Union law while preserving the security and commercial interests of the entity concerned.**

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 **to ensure effectiveness of the support action**.

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 **three** ~~one~~ month**s** from the end of the support action, the users shall provide **the** Commission**,** ~~and~~ ENISA**, the CSIRTs network and, where appropiate, EU-CyCLONe** 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**, on a regular basis and at least once per year,** 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[1], the support under this Regulation for 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 **that the services included in** the EU Cybersecurity Reserve **are such that the 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;

---

[1] 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).

(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**, if so required by the Member State**;

(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 **inform the Council and** coordinate with the High Representative about the requests received and the implementation of the support granted to third countries from the EU Cybersecurity Reserve.

*Article 17a) ~~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[1], the support under this Regulation for responding to such incidents shall complement actions under and be 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.**

# Chapter IV

## *CYBERSECURITY INCIDENT REVIEW MECHANISM*

*Article 18*

**Cybersecurity Incident Review Mechanism**

---

1 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).

1. **After consulting Member States concerned, and ~~A~~a**t 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, **and in close cooperation with the Member State(s) concerned,** 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**, after consulting Member States concerned**. 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~~ **Cybersecurity Alert System**, 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';

(b) 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[1] 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:

"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.

---

[1] 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).

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~~ **Cybersecurity Alert System** 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* |