Council of the European Union
General Secretariat

Interinstitutional files:
2023/0109 (COD)

Brussels, 15 December 2023

WK 17037/2023 INIT

LIMITE

CYBER
CODEC

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:	General Secretariat of the Council
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 - draft mandate

Delegations will find in the Annex a draft mandate on the above legislative proposal.

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, and amending Regulation (EU) 2021/694

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.

---

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

(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 **sectors of high** critical**ity** or ~~**highly**~~ **other** 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[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 **and inital recovery from** significant and large-scale cybersecurity incidents. **Building on the existing structures and in close cooperation with them,** ~~**T**~~**t**he Union should also increase its capacities in these areas, notably as regards the collection and analysis of data on cybersecurity threats and incidents.

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

(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 **to** strengthen~~ed~~ solidarity at Union level to better detect, prepare for and respond to cybersecurity threats and incidents**, in particular by reinforcing the capabilities of existing structures such as the CSIRTs network**. 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].

---

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)

(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 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 **and large-scale-equivalent** cybersecurity incidents. Therefore a pan-European infrastructure of **Cyber Hubs ~~[SOCs]~~** (European Cyber**security** ~~Shield~~ **Alert System**) should be **~~deployed~~ established** to build ~~and enhance~~ **common coordinated** detection and situational awareness capabilities **~~and enhance the existing ones~~**; a Cybersecurity Emergency Mechanism should be established to support Member States **upon their request** in preparing for, responding to, and **~~immediate~~ initially** 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. **The actions under this Regulation should be conducted with due respect for Member States' competences and should complement and not duplicate ~~duplication of~~ the activities conducted by the CSIRT network, EU-CyCLONe and the NIS Cooperation Group, established in Directive (EU) 2022/2555 ~~of the European Parliament and of the Council~~**. These actions shall be without prejudice to Articles 107 and 108 of the Treaty on the Functioning of the European Union ('TFEU').

---

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

(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**security** ~~Shield~~ **Alert System** and the Cyber Emergency Mechanism under Specific Objective 3 of **the Digital Europe Programme (**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 **and coordination** on cybersecurity. **The European Cybersecurity Alert System could play an important operational role in supporting Member States in anticipating and protecting against cyber threats, and the EU Cybersecurity Reserve could play an important operational role in supporting Member States, ~~EUIBAs~~Union institutions, bodies and agencies, and DEP-associated third countries in responding to and mitigating the impacts of significant incidents, ~~and~~ large-scale cybersecurity incidents, and ~~equivalent~~ large-scale equivalent cybersecurity incidents. Those impacts could include considerable material or non-material damage and serious public security and safety risks. In light of the specific operational roles that the Cybersecurity Alert System and the EU Cybersecurity Reserve could play, this Regulation should amend Regulation (EU) 2021/694 as regards the participation of legal entities that are established in the Union but are controlled from third countries, in cases where there is a real risk that the necessary and sufficient tools, infrastructures and services, or technology, expertise and capacity, will not be available in the Union and the benefits of including such entities outweigh the security risk. ~~Recognising the critical role that the EU Cybersecurity Reserve could play to support Member States in responding to and mitigating the impacts of significant and large-scale cybersecurity incidents, which impacts may include considerable material and non-material damage and serious public security and safety risks, this Regulation should amend Regulation (EU) 2021/694 in relation to the participation of trusted providers that are established in the Union but are~~

[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).

~~controlled from third countries, in cases where the necessary technology and expertise is not available in the Union and subject to an appropriate risk assessment. This will be complemented by t~~**T**he specific conditions under which financial support may be granted for ~~those~~ actions **implementing the Cybersecurity Alert System and the EU Cybersecurity Reserve** 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) **While prevention and preparedness measures are essential to enhance the resilience of the Union in facing ~~serious~~ significant incidents, large-scale cybersecurity incidents, and large-scale-equivalent cybersecurity incidents, the occurrence, timing and magnitude of such incidents are by their nature unpredictable. The financial resources required to ensure an adequate response can vary significantly from year to year and should be capable of being made available immediately. Reconciling the budgetary principle of predictability with the necessity to react rapidly to new needs therefore requires adaptation of the financial implementation of the work programmes. Consquently, it is appropriate to authorise carry-over of unusued appropriations, limited to the following year**

and solely to the Cybersecurity Emergency Mechanism, in addition to the carry-over of appropriations authorised under Article 12(4) of the Financial Regulation.

~~**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 Cyber Hubs SOCs] should be deployed established ('tThe** European Cyber**security** ~~Shield~~ **Alert System'), comprising consists** of several interoperating cross-border **Cyber Hubs platforms**, each grouping together **three or more several national SOC Hubs National Cyber Hubs**. That infrastructure should serve national and Union cybersecurity interests and needs, leveraging state-of-the-art technology for advanced ~~**data**~~ collection **of relevant and, where appropriate, anonymised data** and analytics tools, enhancing **coordinated** 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].

~~[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).~~

(13) **Participation in the European ~~Cyber Shield~~ Cybersecurity Alert System ~~should be~~ is voluntary for Member States.** Each Member State **that decides to join the European ~~Cyber Shield~~ Cybersecurity Alert System** should designate a **~~National SOC hub~~ National Cyber Hub.** ~~public body at national level tasked with coordinating cyber threat detection activities in that Member State.~~ **~~Member States should be able to designate an existing entity to conduct the functions of the single [National SOC hub], or establish a new one~~ Thisese National Cyber Hub ~~National SOCs hubs~~ could be an entity mandated under Union law for cyber security related tasks such as CSIRTs (Computer Security Incident Reponse Teams)**, **a national cyber crisis management authority or other competent authority designated or established under ~~Article 10 8 of~~ Directive 2022/2555, or another entity acting under the authority of the Member State which has ~~another entity having as~~** ~~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, **in particular, be capable of detecting malicious events, cyber ~~security~~ threats and incidents, ~~aggregating and analysing data~~ through data relevant to cyber threats and incidents, including by using ~~in particular~~ state-of-the-art technologies. Member States should be able to decide to designate an existing entity to conduct the functions of National Cyber Hub ~~National SOC hub~~, or establish a new one consisting of one or more entities under the authority of a Member State. ~~Member States should also be able to decide to designate, at the national level, different entities to carry out the different functionalities of the [National SOC hub], while only having one National SOC hub.~~ The Cybersecurity Alert System should enhance the CSIRTs network's capabilities ~~and that would be~~ by sharing relevant information~~ed appropriately with the CSIRT network~~ in order to support the network and cooperate with it in conducting its activities. ~~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, at the national level, different entities to carry out the different functionalities of the [National SOC hub].~~**

(14) As part of the European Cyber**security Alert System** ~~Shield~~, a number of **Cross Border Cyber Hubs** **[**~~Cross-border Cybersecurity Operations Centres ('Cross-border SOCs'~~ **collaboration platforms)]** should be established. These should bring together **National Cyber Hubs** ~~**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 Cyber Hubs'** ~~**Cross-border SOCs'**~~ **collaboration platforms** 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 **relevant and, where appropriate, anonymised information** ~~**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**, including the CSIRTs network**.

(14a) A Member State selected by the European Cybersecurity Competence Centre (ECCC) following a call for expression of interest to set up a National Cyber Hub ~~**National SOC Hub**~~ **or enhance the capabilities of an existing one, should** ~~**jointly**~~ **purchase relevant tools, infrastructures and services jointly with the ECCC. Such a Member State should be eligible to receive a grant to operate the tools, infrastructures and services. A Hosting Consortium consisting of at least three Member States, which has been selected by the ECCC following a call for expression of interest to set up a Cross Border Cyber Hub** ~~**Cross-border collaboration SOC collaboration platform**~~ **or enhance the capabilities of an existing one, should** ~~**jointly**~~ **purchase relevant tools, infrastructures and services jointly with the ECCC. Such a Hosting Consortium should be eligible to receive a grant to operate the tools, infrastructures and services.** ~~**In accordance with Article 165(2) of Regulation EU 2018/1046, and Article 90 of Decision no GB/2023/1 of the Governing Board of the ECCC, the**~~ **The procurement procedure to purchase the relevant tools, infrastructures and services should be carried out jointly by the ECCC and relevant contracting authorities from the Member States selected following these calls for expressions of interest. This procurement should be in accordance with Article 165(2) of Regulation EU 2018/1046, and Article 90 of Decision no GB/2023/1 of the Governing Board of the ECCC.**

Private entities should therefore not be eligible to participate in the calls for expression of interest to jointly purchase tools, infrastructures and services with the ECCC, or to receive grants to operate those tools, infrastructures and services. However, the Member States should have the possibility to involve private entities in the setting up, enhancement and operation of their National Cyber Hubs ~~National SOC Hubs~~ and Cross Border Cyber Hub ~~Cross-border SOCs collaboration Platforms~~ in other ways which they deem appropriate, in compliance with national and Union law. ~~For providing support to National Cyber Hub entities~~, private entities could also be eligible to receive Union funding in accordance with Regulation (EU) 2021/887 in order to provide support to National Cyber Hubs.

(14b) In order to enhance cyber threat detection and situational awareness in the Union, a Member State which is selected following a call for expression of interest to set up a National Cyber Hub ~~SOC~~ hub or enhance the capabilities of an existing one, should commit to apply to participate in a Cross Border Cyber Hub ~~Cross-border SOC collaboration Platform]~~ ~~within two years from the date on which the tools, infrastructures and services are acquired, or on which it receives grant funding, whichever occurs sooner~~. If a Member State is not a participant in a Cross-border Cyber Hub ~~collaboration Platform~~ within two years from the date on which the tools, infrastructures and services are acquired, or on which it receives grant funding, whichever occurs sooner ~~by this date~~, it should not be eligible to participate in further Union support actions to enhance the capabilities of its National Cyber Hub ~~National SOC hub~~ provided for in Chapter II of this Regulation. In such cases, ~~. E~~ entities from Member States could ~~in any case~~ still participate in calls for proposals on other topics under DEP or other European funding programs, including calls on capacities for cyber detection and information sharing, provided that those entities meet the eligibility criteria established in the programs.

(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 **EU Cybersecurity Alert System** ~~Cross Border Cyber Hub [Cross-border SOCs collaboration platform]~~ should constitute a new capability that is complementary to the CSIRTs network **by**

contributing to building a Union situational awareness allowing the reinforcement of ~~and should reinforce~~ the capabilities of the latter. Cross Border Cyber Hubs ~~[The cross-border support collaboration platform]~~ should coordinate and ~~will~~ cooperate closely with the CSIRTs Network. They should act ~~it~~, by pooling **data** and sharing **relevant and, where appropriate, anonymized information ~~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 Cyber Hub ~~[Cross-border SOCs collaboration platform]~~** 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~~ stakeholders** (**~~e.g.,~~ such as** Computer Emergency Response Teams ('CERTs'), CSIRTs, Information Sharing and Analysis Centers ('ISACs'), operators of critical infrastructures). **Members of the Hosting Consortium should specify in the consortium agreement the relevant information to be shared among the participants of the Cross Border Cyber Hub ~~[Cross border SOCs collaboration platform]~~.** The information exchanged among participants in a ~~[~~Cross-border **Cyber Hub ~~SOC]~~** could include **for instance** data from networks and sensors, threat intelligence feeds, indicators of compromise, and contextualised information about incidents, threats**,** ~~and~~ vulnerabilities **and near misses, techniques and procedures, adversarial tactics, threat actors specific information, cybersecurity alerts and recommendations regarding the configuration of cybersecurity tools to detect cyberattacks**. In addition, **Cross Border Cyber Hubs ~~[Cross-border SOCs collaboration platforms]~~** should also enter into cooperation agreements with other **Cross Border Cyber Hubs ~~[Cross-border SOCs collaboration platforms]~~**.

(16a) The Cross Border Cyber Hubs ~~[Cross-border SOCs collaboration platforms]~~ and the CSIRTs network should cooperate closely to ensure synergies and complementarity of activities. For that purpose, they should agree on procedural arrangements on cooperation and sharing of relevant information. This could include sharing of relevant information on cyber threats, significant cybersecurity incidents and ensuring that experiences with state-of-the-art tools, notably Artificial Intelligence and data analytics technology, used within the

Cross Border Cyber Hubs ~~[Cross-border SOCs collaboration platforms]~~ is shared with the CSIRTs network.

(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. **Directive (EU) 2022/2555 also establishes the CSIRTs network to promote swift and effective operational cooperation among all Member States. To ensure situational awareness and strenghten solidarity, in situations where Cross Border Cyber Hubs ~~[Cross-border SOCs collaboration platforms]~~ obtain information related to a potential or ongoing large-scale cybersecurity incident, they should provide relevant information to the CSIRTs network and inform, as an early warning, EU-CyCLONe. ~~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 and 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**security Alert System** ~~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~~ causes ~~and impacts of cybersecurity~~ **of detected cyber threats and cybersecurity risks, should take into account existing work done in the context of the implementation of Directive (EU) 2022/2555.**

(19) In order to enable the exchange of **information** ~~data~~ on cybersecurity threats from various sources, on a large-scale basis, in a trusted environment, entities participating in the European Cyber**security Alert System** ~~Shield~~ should be equipped with state-of-the-art and highly-secure tools, equipment and infrastructures. **The Commission, after consulting the CSIRTs Network, EU-CyCLONe, the NIS Cooperation Group and ENISA, should be able to issue guidance in this respect, with due respect to national defence and security interests.** 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, **analysing** ~~correlating~~, sharing and exchanging **relevant data and information**, the European ~~Cyber Shield~~ **Cybersecurity Alert System** should enhance the Union's technological sovereignty. The pooling of high-quality curated data ~~should~~ **could** 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**[13]**.**~~

(21) While the European Cyber**security Alert System** ~~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**~~

[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).

~~'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 Cybersecurity Alert System 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 and taking stock of any development in that area.~~

(22) Information sharing among participants of the European Cyber**security Alert System** ~~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.

(22a) Information sharing among participants of the European Cybersecurity Alert System could take place using non-disclosure agreements, or informal ~~non-disclosure agreements~~ guidance on information distribution such as the traffic light protocol. The ~~t~~Traffic L~~l~~ight P~~p~~rotocol (TLP) is to be understood as a means to provide information about any limitations with regard to the further spreading of information. It is used in almost all CSIRTs and in some information analysis and sharing centres.

~~**(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, **namely the Cyber Emergency Mechanism,** to improve the Union's resilience to significant**,** ~~**and**~~ large-scale **and large-scale-equivalent** cybersecurity incidents and complement Member States'

actions through emergency financial support for preparedness, response and **initial** ~~**immediate**~~ recovery of essential services. **As the full recovery from an incident is a comprehensive process of restoring functioning of the entity affected by the incident to the state from before the incident and could be a long process that entails significant costs, the support from the EU Cybersecurity Reserve should be limited to the initial stage of the recovery process, leading to the restoration of basic functionalities of the systems.** 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 complemenng their own measures and resources, and other existing support options in case of response to and ~~**immediate**~~ **initial** 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[14] ~~**and Hybrid Rapid Response Teams**~~. It should address the need to ensure that specialised means are available to support preparedness**,** ~~**and**~~ response **and recovery** to cybersecurity incidents across the Union and in **DEP-associated** third countries.

(26) This ~~**instrument**~~ **Regulation** is without prejudice to procedures and frameworks to coordinate crisis response at Union level, in particular the **Union Civil Protection Mechanism established under Decision No 1313/2013/EU of the European Parliament and of the Council** ~~**UCPM**~~[15], **the EU Integrated Political Crisis**

---

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).

Response Arrangements under Council Implementing Decision (EU) 2018/1993 ~~IPCR~~[16] (IPCR Arrangements), Commission Recommendation 2017/1584[17] and Directive (EU) 2022/2555. ~~**It may**~~**Support provided under the Cyber Emergency Mechanism can complement assistance provided in the context of the Common Foreign and Security Policy and the Common Security and Defence Policy, including through the Cyber Rapid Response Teams, taking into account the civilian nature of the Mechanism. Support provided under the Cyber Emergency Mechanism can ~~contribute to or~~** complement actions implemented in the context of Article 42(7) **~~of~~** TEU**, including assistance provided by one Member State to another Member State,** or **form part of the joint response between the Union and Member States** in situations ~~**defined**~~ **referred to** in Article 222 ~~**of**~~ TFEU. The ~~**use**~~ **implementation** of this ~~**instrument**~~ **Regulation** should also be coordinated with the implementation of **measures under the** 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**s**

and the Commission and, where relevant, ENISA and the ECCC, 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-

---

16 **Council Implementing Decision (EU) 2018/1993 of 11 December 2018 on the EU Integrated Political Crisis Response Arrangements (OJ L 320, 17.12.2018, p. 28).** ~~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.~~

17 **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).**

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~~ **initial** recovery ~~and/~~or restore the **basic functionalities** ~~functioning~~ of ~~essential~~ **the** services **provided by entities operating in sectors of high criticality or other critical sectors**.

(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 **of high criticality** identified pursuant to Directive (EU) 2022/2555 in a coordinated manner**, including through exercise and training**. For this purpose, the Commission, with the support of ENISA**,** and ~~in cooperation with~~ **after consulting** the NIS Cooperation Group established by Directive (EU) 2022/2555 **and EU-CyCLONe**, 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[18]. 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 **of high criticality and other 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~~ **initial** 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 **technical** assistance provided by **a** Member State~~s~~ to **another** ~~a~~ Member State affected by a significant or large-scale cybersecurity incident, including by ~~the~~ CSIRTs ~~network~~ **as** ~~set out~~ **referred to** in Article **11(3) point (g)** ~~5~~ of Directive (EU) 2022/2555. Member States providing **such** 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.

(32a) Given the essential role that private companies play in the detection, preparedness and response to ~~major~~ large-scale cybersecur~~ityirty~~ incidents, a framework for ~~a~~ voluntary pro-bono cooperation could be established at EU level, consisting of providers willing to offer services without remuneration in cases of large-scale and large-scale equivalent cybersecurity incidents and crises. Such framework could be established by ENISA in cooperation with the EU-

[18] 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

CyCLONe and should be compliant with the criteria applicable to trusted providers under this regulation ~~and could include requirements~~ including in relation to the trustworthiness of companies, their experience as well as the ability to handle sensitive information in a secure manner.

(33) **~~A~~ As part of the Cyber Emergency Mechanism, a** Union-level Cybersecurity Reserve should gradually be set up, consisting of services from **trusted ~~private~~** providers **~~of managed security services~~** to support response and **~~immediate~~ initiate** recovery actions in cases of significant**, ~~and~~** large-scale **or large-scale-equivalent** cybersecurity incidents **affecting Member States, Union institutions, bodies and agencies, or DEP-associated third countries.** The EU Cybersecurity Reserve should ensure the availability and readiness of services**. It should therefore include services that are committed in advance, including for instance capacities that are on stand-by and deployable at short notice. In order to ensure the effectivee use of Union funding, pre-committed services should be convertible into preparedness services closely related to incident response, in the event that those pre-committed services cannot be used for incident response.** The services from the EU Cybersecurity Reserve should serve to support national authorities in providing assistance to affected entities operating in **sectors of high** critical**ity** or **~~highly~~ other** critical sectors as a complement to their own actions at national level. When requesting support from the EU Cybersecurity Reserve, **applicants for support ~~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 **from the applicant**. **Requests for support from the EU Cybersecurity Reserve from Member States' cyber crisis management authorities and CSIRTs, CERT-EU on behalf of the and Union institution, bodies and agencies, should be assessed by ENISA, in cases where ENISA has been entrusted with the administration and operation of the EU Cybersecurity Reserve. To facilitate the submission and assessment of requests for support, ENISA could set up a secure platform. Requests for support from DEP- associated third countries should be assessed by the Commission. ~~The CSIRTs network~~ EU-CyCLONe ~~established in Directive EU 2022/2555~~ ~~can~~ should, where relevant, be able to advise ENISA or the Commission in assessing ~~reviewing~~ requests for support from the EU Cybersecurity Reserve**. The services from the EU Cybersecurity Reserve may also serve to support Union institutions, bodies and agencies, under similar conditions. **~~The~~**

It is important to take into account the European Cybersecurity Skills Framework (ECSF) ~~should be taken into account~~ when procuring the services for the reserve.

(33a) ~~Having overall responsibility for the implementation of the EU Cybersecurity Reserve, the Commission should be the contracting authority for the procurement of services to establish the EU Cybersecurity Reserve, insofar as the operation and administration of those services has not been entrusted to ENISA. Insofar as as the operation and administration of the EU Cybersecurity Reserve has been entrusted, in full or in part, to ENISA,~~ The Commission should have ~~the~~ overall responsibility for the functioning of the EU Cybersecurity Reserve. Given the extensive experience gained by ENISA with the cybersecurity support action, ENISA is the most suitable Agency to implement the EU Cybersecurity Reserve, therefore the Commission should strongly consider entrusting ENISA ~~the Commission should entrust ENISA~~ with the operation and administration of the EU Cybersecurity Reserve. ENISA should ~~may~~ be the contracting authority for those services with whose operation and administration it has been entrusted. ENISA should also assess requests for support from the EU Cybersecurity Reserve for such services, with the exception of requests from DEP-associated third countries where a specific procedure should apply.The procurement procedures to establish the EU Cybersecurity Reserve should be conducted in accordance with Regulation EU 2018/1046. When evaluating tenders for the purpose of establishing the EU Cybersecurity Reserve, external experts from the Member States ~~can should be~~ are able to assist the evaluation committee pursuant to Article 150(3) of that Regulation. The resulting contracts, including any framework contract and specific contracts implementing a framework contract, should be signed by the contracting authority and the selected service provider. In addition, the service provider and the user to which the support under the EU Cybersecurity Reserve is provided could sign specific agreements which specify the way in which the services are to be provided and the liability conditions in case of damage caused by the services of the EU Cybersecurity Reserve. ~~Where the user uses such services to support an affected entity,~~ The ~~is~~ way in which support shall be provided and the liability conditions in respect of the affected entities may be determined by national law, by the specific agreement between the service provider and the user, or by a specific agreement

between the specific provider, the user and the affected entity. ~~In addition, the service provider and the user to which the support under the EU Cybersecurity Reserve is provided should sign specific agreements which specify the way in which the services are to be provided to the affected entities, and the liability conditions towards those entities in case of damage caused by the services of the EU Cybersecurity Reserve.~~ Appropriate agreements should be established between the parties involved clarifying roles and responsibilities and the protection of information through non-disclosure agreements. ~~These agreements should stipulate that the Commission, and ENISA should bear no contractual liability towards the affected entities for any damages caused by the services.~~ In order ~~to ensure that these agreements between the service providers and the users are available when needed, so as~~ to allow the services to be deployed quickly in case of a request for support from the EU Cybersecurity Reserve, they may be based on templates prepared by ENISA, after consulting Member States.

(33b) **~~Due regard should be given to the role of the~~ Member States should have a key role in the constitution, deployment and post-deployment ~~of the implementation~~ of the EU Cybersecurity Reserve. As Regulation (EU) 2021/694 is the relevant basic act for actions implementing the EU Cybersecurity Reserve, the actions under the EU Cybersecurity Reserve should be provided for in the relevant work programmes referred to in Article 24 of Regulation (EU) 2021/694. In accordance with Article 24(6) of Regulation (EU) 2021/694, these work programmes should be adopted by the Commission by means of implementing acts in accordance with the examination procedure referred to in Article 5 of Regulation (EU) No 182/2011. Furthermore, ~~by virtue of cooperating with~~ the Commission, in cooperation with EU CyCLONe, ENISA and the NIS Cooperation Group, ~~the Commission~~ should ~~ensure~~ determine ~~that~~ the ~~views of Member States~~ priorities and the evolution of the EU Cybersecurity Reserve ~~are taken into account.~~**

(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 **sectors of high** critical**ity** or ~~highly~~ **other** critical sectors are met. **In order to address specific needs of Member States, when procuring services for the EU Cybersecurity Reserve,**

the contracting authority should, where appropriate, develop additional selection criteria to those laid down in this Regulation.

(35) To support the establishment of the EU Cybersecurity Reserve, the **Commission ~~could consider~~ should request ~~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, with due respect of Member States competences~~, with the approval of the Member States concerned,** should be able to ask ENISA to review and assess threats, **known exploitable** 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 the Member State concerned, ~~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 **to ~~and feed into the work of the~~** EU-CyCLONe, the CSIRTs network, and the Commission **and should feed into their work as well as that of ENISA**. When the incident relates to a **DEP-associated** third country, it **should ~~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**, and particularly its internal market and industry,** as a whole. **Such activities could further contribute to the EU cyber diplomacy.** Therefore, **DEP-associated** third countries ~~**associated to the DEP**~~ may be supported from the EU Cybersecurity Reserve, **in all or part of their territories**, where this is provided for in the ~~**respective association relevant**~~ agreement ~~**or Association Council decision**~~ **through which** ~~**to**~~ **the third country is associated** to DEP. ~~**The Commission should therefore cooperate with the High Representative in respect of such support, noting, that**~~ ~~**The CSIRT Network established in Directive EU 2022/2555 and can advise the Commission in reviewing requests for support from the EU Cybersecurity Reserve. Iin certain cases, support provided to DEP-associated third countries could complement assistance provided in the context of the Common Foreign and Security Policy and the Common Security and Defence Policy.**~~ ~~**Such activities could further contribute to the EU cyber diplomacy. The Commission should therefore cooperate with the High Representative in respect of such support.**~~ The funding for **DEP**-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~~ **initiate** 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 **DEP-associated** third countries ~~**associated to DEP**~~. **DEP-associated third countries should be entitled to request the service from the EU Cybersecurity Reserve when the entities targeted and for which they request support from the EU Cybersecurity Reserve, are entities operating in the sectors referred in the Annex I and II of Directive 2022/2555 and when the incidents detected lead to an operational overrun or might have spill over effects in the Union. Support provided to DEP-associated third countries could affect the availability of the Reserve to support the Member States and Union institutions, bodies and agencies. It should be consistent with the criterion for prioritising support to Member States, Union institutions, bodies and agencies, and DEP-associated third countries. It may also affect relations with third countries, including in the context for the Common Foreign and Security Policy and Common Defence and Security Policy. Accordingly, it is appropriate that the Council reserves to itself the right to exercise implementing powers to authorise and specify the time period during which such support can**

be provided. The Commission should take into account any opinion provided by ENISA or the High Representative in respect of such support.

(37a) Without prejudice to the rules relating to the Union's annual budget under the Treaties, the Commission should take into account the obligations arising from this Regulation when assessing the budgeting and staffing needs of ENISA.

(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 Cybersecurity Alert System 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 **establishment** ~~**deployment**~~ of a pan-European infrastructure of **Cyber Hubs** ~~**[Security Operations Centres]**~~ ('European ~~Cyber Shield~~ **Cybersecurity Alert System**') to build and enhance ~~**common**~~ **coordinated** detection and **common** situational awareness capabilities;

   (b) the creation of a Cybersecurity Emergency Mechanism to support Member States **and other users** in preparing for, responding to, **mitigating the impact of** and **inititating** ~~immediate~~ recovery from significant**,** ~~**and**~~ large-scale **and large-scale** equivalent 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**~~ **of** strengthen**ing** solidarity at Union level **and enhanceing Member States cyber resilience, so as 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,** through **the** following specific objectives:

   (a) to strengthen ~~**common**~~ **coordinated** Union detection **capacities** and **common** 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 **sectors of high** critical**ity** and ~~**highly**~~ **other** critical sectors, across the Union and strengthen solidarity by developing **enhanced** ~~common~~ response **and recovery** capacities **to handle** ~~against~~ significant**,** ~~**or**~~ large-scale or **large-scale-equivalent** cybersecurity incidents, including **the possibility of** ~~**by**~~ making Union cybersecurity incident response support available for **DEP-associated** third countries ~~associated to the Digital Europe Programme ('DEP')~~;

(c) to enhance Union resilience and contribute to effective response by, **upon request of the Member States,** reviewing and assessing significant or large-scale incidents, including drawing lessons learned and, where appropriate, recommendations, ~~**upon request and**~~ **with the approval of the** ~~**in coordination with**~~ **Member States concerned.**

2(a) The actions under this Regulation shall be conducted with due respect to the Member States' competences and shall be complementary to the activities carried out by the CSIRTs network, NIS Cooperation Group, ~~**CSIRTs network**~~ **and EU-CyCLONe.**

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 safeguarding national security.** ~~and the prevention, investigation, detection and prosecution of criminal offences.~~ **In particular**, **national security remains the sole responsibility of each Member States.**

4. ~~**Without prejudice to Article 346 TFEU, the**~~ **This regulation is without prejudice to Article 346 TFEU and all exchange** ~~**under this Regulation**~~ **of information that is confidential pursuant to Union or national rules shall be limited to that which is relevant and proportionate to the purpose of that exchange. The exchange of such information under this Regulation shall 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. It shall not entail the supply of information the disclosure of which would be contrary to the Member States' essential interests of national security, public security or defence.**

Article 2

Definitions

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

(-1) National Cyber Hub ~~**'National Security Operations Centre Hub' ("National SOC hub")**~~ **means a**~~**n**~~ **single entity designated by and acting under the authority of a Member State, which may be a CSIRT, a national cyber crisis management**

authority or other competent authority designated or established under Directive 2022/2555 or ~~a new~~ another entity, under the authority of a Member State, ~~and~~ 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 to contribute~~ing~~ to a Cross Border Cyber Hub ~~[Cross-border SOC collaboration 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 Cyber Hub ~~[‘Cross-border Security Operations Centre collaboration Platform’ (“Cross-border SOC collaboration Platform”)]~~ ~~for the purpose of this Regulation~~** means a multi-country platform, **established by a written consortium agreeement** that brings together in a coordinated network structure **National Cyber Hubs ~~Nnational SOCs Hubs~~** from at least three Member States ~~who form a Hosting Consortium~~, and that is designed to **enhance the monitoring, detection and analysis** ~~prevent~~ **of** cyber threats ~~and~~ **to prevent** incidents and to support the production of **cyber threat** ~~high-quality~~ intelligence, notably through the exchange of **relevant and, where appropriate, anonymized information ~~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[19];~~

(3) **‘Hosting Consortium’** means a consortium composed of participating **Member S**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 Cyber Hub ~~[Cross-border SOC collaboration Platform;]~~**

---

19 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).

(3a) 'CSIRT' means a CSIRT designated or established pursuant to Article 10 of Directive (EU) 2022/2555 .

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

(5) '**entities operating in sectors of high criticality or ~~highly~~ other 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;

(8aa): 'large-scale-equivalent cybersecurity incident' means, in the case of Union institutions, bodies and agencies, a major incident as defined in Article 3 point (8) of [EUIBAs Regulation] and, in the case of DEP-associated third countries, an incident which causes a level of disruption that exceeds a DEP-associated third country's capacity to respond to it ~~or which has a significant impact on at least two DEP-associated third countries'~~

~~(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 .~~

(8c) 'DEP-associated third country' means a third country which is party to an agreement with the Union allowing for its participation in the Digital Europe Programme pursuant to Article 10 of Regulation (EU) 2021/694;

(8d) 'contracting authority' means the Commission or, to the extent that operation and administration of the EU Cybersecurity Reserve has been entrusted to ENISA under Article 12(6) of this Regulation, ENISA.

Chapter II

THE EUROPEAN ~~CYBER SHIELD~~ CYBERSECURITY ALERT SYSTEM

Article 3

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

1. **A~~n interconnected~~** pan-European infrastructure **that consists** of **National Cyber Hubs ~~National SOC hubs~~ and Cross Border Cyber Hubs ~~[Cross-border SOC collaboration platforms]~~ joining on a voluntary basis,** ~~Security Operations Centres ('European Cyber Shield~~ **the European Cybersecurity Alert System**[2]~~)~~ shall be established to **support the** develop**ment of** advanced capabilities for the Union to **enhance** detect**ion**, **analysis** and **data** process**ing ~~data~~ capabilities** 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) contribute to better protection and response to cyber threats ~~**and incidents**~~ **by supporting and cooperating with, and reinforcing the capacities of, relevant entities, in particular CSIRTs, the CSIRTs network, EU-CyCLONe and the** ~~**such as**~~ **competent authorities designated or established pursuant to Article 8 of Directive (EU) 2022/2555**;

(a) pool **information on cyber threats and incidents from various sources within the Cross Border Cyber Hubs** ~~**[Cross-border SOCs collaboration platforms] data**~~ and share **analysed or aggregated information** ~~**data on cyber threats and incidents from various sources**~~ through **Cross Border Cyber Hubs** ~~**[Cross-border SOCs collaboration platforms]**~~;

(b) ~~**produce share**~~ **collect** high-quality, ~~**actionable**~~ information and cyber threat intelligence, through the use of state-of-the art tools **and advanced technologies** ~~**such as**~~, notably ~~**Aa**~~artificial ~~**Ii**~~ntelligence and data analytics~~**, and share that information and cyber threat intelligence** technologies~~;

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

(d) contribute to **enhanced** ~~faster~~ **coordinated** detection of cyber threats and **common** situational awareness across the Union**, and to the issuing of** ~~**cybersecurity**~~ **alerts** ~~**to relevant entities**~~;

(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 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 Cyber Hubs ~~National Security Operations Centres Hubs~~

1. ~~In order~~ **Where a Member State decides** to **voluntarily** participate in the European ~~Cyber Shield~~ **Cybersecurity Alert System**, ~~each Member State~~ **it** shall **~~appoint~~ designate a single National Cyber Hub ~~National SOC hub one or more CSIRTs or other entities~~ exercising the functions as defined in Article 2 (~~-1~~) ~~to act as a~~ ~~[National SOC hub]~~ for the purposes of this Regulation.** ~~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, infrastructures and serviceswith 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~~ **Article 8a paragraph 1** shall commit to apply **for ~~their~~ its National Cyber Hub ~~National SOC hubs~~** to participate in a **Cross Border Cyber Hub ~~[Cross-border SOC collaboration Platform]~~** ~~within two years from the date on which the tools, infrastructures and servicesare 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~~

~~**collaboration Platform]** by that time, **the Member State** it shall not be eligible for additional Union support under this **Chapter** Regulation~~.

Article 5

Cross-border Cyber Hubs ~~Security Operations Centres collaboration Platforms~~

1. A Hosting Consortium consisting of at least three Member States, ~~represented by National SOCs~~, committed to **ensuring that their National Cyber Hubs ~~National SOC hubs work~~s** ~~working~~ together to coordinate their cyber-detection and threat monitoring activities shall be eligible to participate in actions to establish a **Cross Border Cyber Hub ~~[Cross-border SOC collaboration 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, infrastructures and serviceswith 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 ~~A~~**a**greement **referred to in Article 8a**.

4. A **Cross Border Cyber Hub ~~[Cross-border SOC collaboration Platform]~~** 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.~~ **The responsibility for compliance of the Cross Border Cyber Hub ~~[Cross-border SOC collaboration Platform]~~ with this Regulation and the hosting and usage agreement shall be determined in the written consortium agreement referred to in paragraph 3.**

5. **A Member State may join an existing Hosting Consortium with the agreement of the Hosting Consortium members. The written consortium agreement referred to in paragraph 3 and the hosting and usage agreement shall be modified accordingly. This shall not affect the ECCC's ownership rights over the tools, infrastructures and services already jointly procured with that Hosting Consortium.**

Article 6

Cooperation and information sharing within and between Cross Border Cyber Hubs ~~[Cross-border SOCs collaboration platforms]~~

1. Members of a Hosting Consortium shall **ensure that their National Cyber Hubs** ~~National SOC hubs~~ exchange**, in accordance with the Consortium Agreement referred to in Article 5(3),** relevant **and where appropriate, anonymized** information among themselves within the **Cross Border Cyber Hub [~~Cross-border SOC collaboration platform]~~** ~~including information relating to cyber threats, near misses, vulnerabilities,~~ **techniques and procedures**~~, indicators of compromise, adversarial tactics~~**, threat-actor-specific information, and** ~~cybersecurity alerts~~ **and recommendations regarding the configuration of cybersecurity tools to detect cyber attacks,** ~~where such information sharing:~~

   (a) **~~aims to~~ fosters and enhances the detection of cyber threats and reinforces the capabilities of the CSIRTs network to prevent and ~~prevent, detect,~~** respond to **~~or recover from~~** incidents or to mitigate their impact;

   (b) enhance**~~s~~** 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~~ **relevant and where appropriate, anonymized information**

referred to in paragraph 1, and the conditions under which that information is to be exchanged**. The agreement may specify that the information shall be exchanged in accordance with national law**;

(b) a governance framework **clarifying and** incentivising the sharing of **relevant and, where appropriate, anonymized** 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 **relevant and, where appropriate, anonymized** information between **Cross Border Cyber Hubs** ~~[Cross-border SOCs **collaboration platforms]**~~, ~~[Cross-border SOCs **collaboration platforms**]~~ **Cross Border Cyber Hubs** shall ensure a high level of interoperability between themselves**. ~~[Cross-border SOCs collaboration platforms]~~ Cross Border Cyber Hubs shall conclude cooperation agreements with one another, specifying interoperbility and information sharing principles among the cross-border Cyber Hubs ~~platforms~~. Cross-border Cyber Hubs ~~SOC collaboration Platforms~~ shall inform the Commission about the agreements concluded**. ~~The Commission, **in cooperation with** ~~ENISA, in cooperation with the ECCC and the CSIRTs network may issue guidance~~ ~~T~~to support establishing interoperability ~~facilitate the interoperability~~ between the Cross Border Cyber Hubs ~~[Cross-border SOCs **collaboration** platforms]. **the Commission may, by means of implementing acts, after consulting the ECCC,** specify**ing the its** 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. **Before submitting those draft implementing acts When preparing that guidance to the committee referred to in Article 21(1), the Commission shall consult the ECCC, the NIS Cooperation group and existing [Cross-border SOC collaboration Platforms].**~~

~~4. [Cross-border SOCs 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-level ~~entities and~~ networks

-1. Cross-border Cyber Hubs SOC collaboration Platforms and the CSIRTs Network shall cooperate closely, in particular for the purpose of sharing information. To that end, they shall agree on procedural arrangements on cooperation and sharing of relevant information.

1. Where the **Cross Border Cyber Hubs** [Cross-border SOCs collaboration platforms] obtain information relating to a potential or ongoing large-scale cybersecurity incident, they shall **ensure** provide **that** relevant information **as well as early warnings are is provided** to **the CSIRTs network, and** EU-=CyCLONe, the CSIRTs network, **and the Commission**, **without undue delay,** in view of their respective crisis management roles in accordance with Directive (EU) 2022/2555**.**

2. The Commission may, issue guidance by means of implementing acts, to determine the on 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 **cyber**security, **including data security, as well as and** physical security of the European Cyber Shield **Cybersecurity Alert System** infrastructure, and shall ensure that the infrastructure shall be **is** 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 **information and** data exchanged through the infrastructure.

2. Member States participating in the European Cyber Shield **Cybersecurity Alert System** shall ensure that the sharing of **relevant and, where appropriate, anonymized** information within the European Cyber Shield **Cybersecurity Alert System** with **any entity other than a public authority or body of a Member State entities which are not Member State public bodies** does not negatively affect the security interests of the Union **or the Member States.**

3. ~~The Commission may~~ **~~adopt implementing acts issue guidance documents laying down technical requirements for Member States to comply with their obligation under clarifying the application of~~** ~~paragraphs 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, When preparing those guidance documents,~~** ~~the Commission,~~ **~~in cooperation with~~** ~~supported by the High Representative, shall take into account relevant defence-level security standards, in order to facilitate cooperation with military actors.~~

Article 8a

Funding of the European Cybersecurity Alert System

1. Following a call for expression of interest, Member States intending to participate in the European Cybersecurity Alert System shall be selected by the European Cybersecurity Competence Centre ('ECCC') to take part in a joint procurement of tools, infrastructures and services with the ECCC, in order to set up National Cyber Hubs ~~National SOC hubs~~, as referred to in Article 4(1), or enhance capabilities of an existing one. The ECCC may award grants to the selected Member States to fund the operation of those tools, infrastructures and services. The Union financial contribution shall cover up to 50% of the acquisition costs of the tools, infrastructures and services, 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, infrastructures and services, the ECCC and the Member State shall conclude a hosting and usage agreement regulating the usage of the tools, infrastructures and services.

2. If a Member State's National Cyber Hub ~~National SOC Hub~~ is not a participant in a Cross Border Cyber Hub [~~Cross-border SOC collaboration platform~~] within two years from the date on which the tools, infrastructures and services were acquired, or on which it received grant funding, whichever occurred sooner, the Member State shall not be eligible for additional Union support under this Chapter until it has joined a Cross Border Cyber Hub [~~Cross-border SOC collaboration platform~~].

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

3a. The ECCC shall prepare, at least every two years, a mapping of the tools, infrastructures and services necessary to establish or enhance National Cyber Hubs and Cross Border Cyber Hubs, and their availability, including from legal entities established or deemed to be established in Member States and controlled by Member States or by nationals of Member States. When preparing the mapping, ECCC shall consult the CSIRTs Network, any existing Cross-border Cyber Hubs, ENISA and the Commission.

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 **and large-scale-equivalent** cybersecurity incidents (the 'Mechanism').

1a. In the case of Member States, the actions provided under the Mechanism shall be provided upon request and shall be complementary to Member States' efforts and actions to prepare for, respond to and recover from cybersecurity incidents.

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

2a. The actions under the Cyber Emergency Mechanism shall be implemented primarily through the ECCC ~~uropean Cybersecurity Industrial, technology and research Competence Centre and the Network of National Coordination Centres~~, in accordance with Regulation (EU) 2021/887 of the European Parliament and of the Council with the exception of actions implementing the EU Cybersecurity Reserve as referred to in Article 10(1)(b), which shall be implemented by the Commission and ENISA.

Article 10

Type of actions

-1. Member States may request to participate ~~may benefit from~~ in the actions ~~referred to in paragraph 1 upon request~~ under the Mechanism.

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

(a) preparedness actions**, namely** ~~including~~**;**

(i) the coordinated preparedness testing of entities operating in **sectors of high criticality** ~~highly critical sectors~~ across the Union **as specified in Article 11**;

(ii) other preparedness actions for entities operating in sectors of high criticality ~~critical~~ and other ~~highly~~ critical sectors, as specified in Article 11a. ~~including those involving exercises and trainings and~~ ;

(b) ~~response~~ actions~~,~~ supporting response to and **initiating** ~~immediate~~ recovery from significant**, ~~and~~** large-scale **and large-scale-equivalent** 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~~**as specified in Article ~~17aa~~ 16a**

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

Article 11

Coordinated preparedness testing of entities

-3. The Mechanism shall support the voluntary coordinated preparedness testing of entities operating in sectors of high criticality.

-2. The coordinated preparedness testing may consist of *preparedness* ***activities, such as penetration testing, and threat assessment.***

-1. Support for preparedness actions under this Article shall be provided to Member States primarily in the form of grants and under the conditions defined in paragraph 4 and in the relevant work programmes referred to in Article 24 of the Digital Europe Programme.

1. For the purpose of supporting the **voluntary** coordinated preparedness testing of entities referred to in Article 10(1), point (a) (i), across the Union, **and with due respect to the Member States competences,** the Commission, after consulting the NIS Cooperation Group and ~~**where appropriate**~~ **EU-CyCLONe** ~~**ENISA**~~, shall identify the sectors, or sub-sectors, concerned, from the Sectors of High Criticality listed in Annex I to Directive (EU) 2022/2555 **for which a call for proposals to award grants may be issued. The participation of** ~~from which~~ **Member States in those calls is voluntary.** ~~**may**~~ ~~**request to participate and to this end**~~ ~~**propose**~~ ~~entities to may be subject to the coordinated preparedness testing.~~,

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

2. The NIS Cooperation Group in cooperation with the Commission, ENISA, ~~and~~ the High Representative~~,~~ **and, within the remit of its mandate, EU-CyCLONe,** shall develop common risk scenarios and methodologies for the **coordinated testing exercises under Article 10 (1), point (a) (i) of this Regulation and, where appropriate** ~~**. The NIS Cooperation Group, in cooperation consultation with Commission, ENISA and the High Representative, may develop common risk scenarios and methodologies**~~ **for other preparedness actions under Article 10(1)(a)(ii).** ~~**EU-CyCLONe should be informed about the risk scenarios and methodologies identified for coordinated preparedness actions and other preparedness actions.**~~

Article 11a

Other preparedness actions

1. The Mechanism shall also support preparedness actions not covered by Article 11 of this Regulation on Coordinated preparedness ~~**testing of**~~ **actions for entities. Such actions shall include preparedness actions for entities in sectors not identified for coordinated testing pursuant to Article 11**~~**,**~~**. Such actions may support** ~~**including those involving**~~ **vulnerability monitoring, exercises and trainings.**

2. Support for preparedness actions under this Article, shall be provided to Member States upon request and primarily in the form of grants and under the conditions defined in the relevant work programmes referred to in Article 24 of Regulation (EU) 2021/694 ~~**the Digital Europe Programme**~~**.**

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**, or large-scale-equivalent** cybersecurity incidents, and ~~immediate~~ **initiating** recovery from such incidents.

2. The EU Cybersecurity Reserve shall consist of response services from trusted providers selected in accordance with the criteria laid down in Article 16. The Reserve ~~**shall also**~~ **may** include pre-committed services. **Where those pre-committed services cannot be used for incident response because no user, as referred as in Article 12(3) has requested the services of the EU Cybersecurity Reserve ~~significant or large-scale cybersecurity incident occurs~~ during the time for which those services are pre-committed, such services shall be convertible into preparedness services closely related to incident response, such as exercises or trainings**. The ~~services~~ **Reserve shall** be deployable **upon request** in all Member States, **Union institutions, bodies and agencies and in DEP-associated third countries referred to in Article 17(1).**

3. **The u~~U~~**sers of the services from the EU Cybersecurity Reserve shall **be the following ~~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) **CERT-EU ~~on behalf of Union institutions, bodies and agencies~~, in accordance with Article 13 of EUIBAs Regulation**.

   (c) ~~Users~~ Competent authorities such as ~~CSIRTs~~ Computer Security Incident Response Teams and cyber crisis management authorities of DEP-associated third countries in accordance with Article 17(3).

4. ~~**Users referred to in paragraph 3, point (a), shall may only 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 sectors of high criticality or highly other critical sectors.**~~

5. ~~The Commission shall have responsibility~~ **have overall responsibility** ~~for the implementation of the EU Cybersecurity Reserve.~~ **~~To that end, t~~The** Commission**, in cooperation with EU CyCLONe, ENISA and 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. **These priorities shall be revised every two years.**

6. The Commission **may ~~shall~~** 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**, at least every two years,** a mapping of the services needed **by the users as referred to in paragraph 3 ~~of Article 12 article 12 (3)~~ points (a) and (b) and their availability**, **including from legal entities established or deemed to be established in Member States and controlled by Member States or by nationals of Member States. When preparing the mapping, ENISA shall consult ~~after consulting~~ ~~Member States~~ the NIS Cooperation Group**, **EU-CyCLONe,** the Commission **and, where applicable, the Interinstitutional Cybersecurity Board**. ENISA shall prepare a similar mapping, after consulting **EU-CyCLONe and** the Commission **and informing the ~~NIS Cooperation Group~~ the Council ~~and the~~**, to identify the needs of **~~DEP-associated third countries eligible for support from the EU Cybersecurity Reserve pursuant to Article 17~~ users referred to in paragraph 3 point (c)**. **~~The Commission~~ ENISA**, where relevant, shall **~~seek the views~~** 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). **When preparing those implementing acts, the Commission shall take into account the mapping referred to in paragraph 7. Before submitting those draft~~ing~~ implementing acts to the committee referred to in Article 21(1), the Commission shall exchange advice and cooperate with the NIS Cooperation Group and ENISA.**

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 **or large-scale-equivalent** cybersecurity incidents.

2. To receive support from the EU Cybersecurity Reserve, the users referred to in Article 12(3) shall **take all appropriate** measures to mitigate the effects of the incident for which the support is requested, including**, where** ~~**appropriate**~~ **relevant,** the provision of direct technical assistance, and other resources to assist the response to the incident, and ~~immediate~~ recovery efforts.

3. Requests for support **shall be transmitted to the contracting authority in the following way:**

   (a) In the case of ~~**from**~~ users referred to in Article 12(3), point (a), of this Regulation**, such requests** 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.

   ~~**3a.**~~ **(b) In the case of users referred to** ~~**Requests for support from users referred to**~~ **in Article 12(3), point (b), of this Regulation such requests shall be transmitted** ~~**to the Commission and ENISA**~~ **by CERT-EU.**

   (c) In the case of users referred to in Article 12(3), point (c), of this Regulation, such requests shall be transmitted via the single point of contact referred to in Article 17(4) of this Regulation.

4. **In the case of request from users referred to in Article 12(3), point (a), of this Regulation,** Member States shall inform the CSIRTs network, and where appropriate EU-CyCLONe, about their **users'** requests for incident response and **initial** ~~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:**

(i) affected Member State(s) and users, including the risk of spill over to another Member State, in the case of users referred to in Article 12(3), point (a), of this Regulation~~. and the planned use of the requested support, including an indication of the estimated needs,;~~

(ii) affected Union institutions, bodies and agencies, in the case of users referred to in Article 12(3), point (b), of this Regulation;

(iii) affected DEP-associated countries, in the case of users referred to in Article 12(3), point (c), of this Regulation;

(aa) information regarding the requested service, including the planned use of the requested support,-including an indication of the estimated needs.

(b) **appropriate** 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~~ **EU-CyCLONe** ~~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. **In the case of requests from users referred to in Article 12(3)(a) and (b), ~~R~~r**equests for support from the EU Cybersecurity Reserve, shall be assessed by **the contracting authority ~~the Commission ENISA. with the support of ENISA or as defined in contribution agreements under Article 12(6), and a~~ A** response shall be transmitted to the users referred to in Article 12(3)**(a) and (b)** without delay **and in any event no later than 72 hours from the submission of the request to ensure effectiveness of the support action**. **~~ENISA~~ The contracting authority may consult EU-CyCLONe during the assessment process. It shall inform the Council and the Commission of the results of the process.**

1a. ~~ENISA~~ The contracting authority shall ensure the confidentiality of the information shared in the course of requesting and providing the services.

2. To prioritise requests, in the case of multiple concurrent requests **from users referred to in Article 12(3),** 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~~ initial** recovery efforts, as referred in Article 13(2) and Article 13(5), point (b).

   (f) the category of user under Article 12(3) of this Regulation, with higher priority given to Member State users, then to Union institutions, bodies and agencies and finally to DEP-associated third countries.

Where operation and administration of the EU Cybersecurity Reserve has been entrusted, in full or in part, to ENISA under Article 12(6) of this Regulation,

ENISA and Commission shall closely cooperate to ~~respond to~~ prioritize requests in line with this paragraph.

3. The EU Cybersecurity Reserve services shall be provided in accordance with specific agreements between the **trusted** ~~service~~ provider and the user to which the support under the EU Cybersecurity Reserve is provided. ~~**Where the user uses such services to support an affected entity in accordance with Article 14(5a) of this Regulation, t**~~**Those services may be provided in accordance with specific agreements between the trusted provider, the user and the affected entity. All ~~Those~~** agreements **referred to in this paragraph** 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, **and the users of the Reserve** 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.

5a. Users may only use the services granted upon their request from the EU Cybersecurity Reserve in order to respond or support response to and initiate recovery from significant incidents, large-scalecybersecurity incidents or large-scale cybersecurity equivalent incidents. They may only use those services in respect of ~~affecting~~:

(a) entities operating in sectors of high criticality or other critical sectors, in the case of users referred to in Article 12(3), points (a) and (c); and

(b) Union institutions, bodies and agencies, in the case of the user referred to in Article 12 (3), point (b).

6. Within **three** ~~one~~ month**s** from the end of ~~**the**~~ **a** support action, ~~**the**~~ **any** user**s that has received support** shall provide a summary report about the service provided, results achieved and lessons learned **as follows:**

(a) users referred to in Article 12(3), point (a), of this Regulation shall provide **the summary report to 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.**~~

(b) users referred to in Article 12(3), point (b), of this Regulation shall provide the summary report **to the Commission, ENISA and the IICB**. ~~**CERT-EU, on behalf of the EUIBA's, shall share such report with the IICB.**~~

(c) users referred to in Article 12 (3) (c) of this Regulation shall ~~**When the user is from a DEP-associated third country as set out in Article 17, such report shall be**~~ share~~d~~ **this report** with the **Commission, which will share it with the Council and the** High Representative.

7. **In case of users refered in Article 12 (3) (a) and (b)** ~~**ENISA The Commission T**~~**the contracting authority** shall report to ~~**the Commission, and the**~~ NIS Cooperation Group**, on a regular basis and at least** ~~**once**~~ **twice per year,** about the use and the results of the support~~, on a regular basis~~ **.**

7a. In case of users refered to in Article 12 (3) (c), the Commission shall report to the Council and inform the High Representative on a regular basis and at least twice per year, about the use and the results of the support.

~~*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[20], 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~~

~~20 **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).**~~

~~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 15a***~~

~~**ENISA in cooperation with EU-CyCLONe may establish a framework for a voluntary cooperation at Union level with managed security service providers for the provision of pro bono services to respond to large-scale and large-scale-equivalent cybersecurity incidents.**~~

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**, when taken as a whole, 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;

   (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**,** **including agreements where relevant,** 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~~;~~**,where required by a Member State;**

(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 **sectors of high** critical**ity** or ~~**highly**~~ **other** 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**;**~~.~~

(k) the provider shall include in the tender, the conversion conditions for any unused incident response service that could be converted into preparedness services closely related to incident response, such as exercises or trainings.

2a. For the purposes of procuring services for the EU Cybersecurity Reserve, the contracting authority shall, where appropriate, develop selection criteria in addition to those referred to in paragraph 2, in close cooperation with Member States.

Article 16a

Mutual ~~A~~assistance

1. The Mechanism shall provide support for technical assistance from one Member State to another Member State affected by a significant or large-scale cybersecurity incident, including in cases referred to in Article 11(3), point (f), of Directive (EU) 2022/2555.

2. The support ~~to~~ for the technical mutual assistance ~~as~~ referred to in paragraph 1 shall be granted in the form of grants and under the conditions defined in the relevant work programmes referred to in Article 24 of the Digital Europe Programme.

Article 17

Support to DEP-associated third countries

1. **A DEP- associated t~~T~~**hird countr**~~ies~~** may request support from the EU Cybersecurity Reserve **~~where~~** ~~Association Agreements concluded regarding their participation in DEP provide for this~~ **~~they are associated or partly associated with DEP and~~ where the agreement, ~~decision or conditions or Association Council decision~~ through which it is associated to DEP provides for participation in the Reserve.**

2. Support from the EU Cybersecurity Reserve **to a DEP-associated third country** shall **~~be approved by the Council in accordance with this Regulation, and shall~~** comply with any specific conditions laid down in the ~~Association Agreements~~ **agreement, ~~or decision or conditions~~** referred to in paragraph 1.

3. Users from **DEP-**associated third countries eligible to receive services from the EU Cybersecurity Reserve shall include competent authorities such as **~~CSIRTs~~ Computer Security Incident and Response Teams** and cyber crisis management authorities.

4. Each **DEP-associated** 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.

~~4a. Requests for support from the EU Cybersecurity Reserve under this Article shall be transmitted to the Commission and ENISA by the single point of contact referred to in Article 17(4).~~

4b. Requests for support from the EU Cybersecurity Reserve under this Article shall be assessed by the Commission ~~and the~~. A response shall be transmitted to the users referred to in Article 12(3) point (c) without undue delay, following the Council's implementing decision refered to in ~~Article~~ paragraph 5a of this Article.

5. **In order to enable the Commission to apply the criteria listed in Article 14(2), ~~to requests from third countries referred to in paragraph 1~~**, **~~pPrior to receiving any support from the EU Cybersecurity Reserve,~~ within three months of the conclusion of the agreement referred to in paragraph 1and in any event prior to receiving any support from the EU cybersecurity reserve, the DEP-associated** 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 **or large-scale-equivalent** cybersecurity incidents, as well as information on responsible national entities, including CSIRTs or equivalent entities, their capabilities and the resources allocated to them. **The DEP-associated third country shall provide updates to this information on a regular basis and at least once per year. The Commission shall share this information with ENISA, EU CyCLONe and the High Representative~~, for~~ the purpose of facilitating the ~~cooperation~~ collaboration referred to in paragraph 6**. **~~Where provisions of~~** Articles **~~13 (5) and (5a) and Article 14 (2) - (5)~~** of this Regulation **~~refer to Member States, they~~** shall apply ***~~mutatis mutandis~~* ~~to DEP-associated~~** third countries **~~as set out in paragraph 1.~~**

5a. Support from the EU Cybersecurity Reserve to a DEP-associated third country shall only be provided after a Council implementing decision has been adopted on

a proposal from the Commission following its assessment under Article 14 (2). The Council implementing decision ~~shall~~ authorise~~ing~~ the Commission to provide support to the DEP-associated third country ~~and~~ shall specify the time period during which such support may be provided. It shall be based on an assessment of the support with regard to the criterion for prioritising multiple requests under Article 14(2)(f) of this Regulation and consistency with the Union's policy towards the DEP-associated third country concerned.

6. The Commission shall **take into account the opinion of ENISA ~~inform NIS Cooperation Group~~ and the High Representative** about the requests received and the implementation of the support granted to **DEP-associated** third countries from the EU Cybersecurity Reserve**, if ~~it is~~ such opinions are provided. ~~consult inform the NIS Cooperation Group Council and cooperatecoordinate with the High Representative~~**

Article 17a) ~~15~~

Coordination with Union crisis management mechanisms

1. ~~In cases w~~Where a significant cybersecurity incident, ~~or~~ a large-scale or large-scale-equivalent cybersecurity incident~~s~~ originates from or results in a disaster~~s~~ as defined in Article 4, point (1), of Decision No 1313/2013/EU[21], the support provided under this Regulation for responding to such incident~~s~~ shall complement actions under, and be without prejudice, to Decision No 1313/2013/EU.

2. In the event of a large-scale or large-scale-equivalent~~, cross border~~ cybersecurity incident where the EU Integrated Political Crisis Response ~~a~~Arrangements under Implementing Decision (EU) 2018/19934 (IPCR Arrangements) are triggered, ~~the~~ support provided under this Regulation for responding to such incident shall be handled in accordance with the relevant ~~protocols and~~ procedures under the IPCR Arrangements.

---

21 ~~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).~~

~~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. ~~After consulting Member States concerned, and~~ **Aa**t the request of ~~the Commission~~, ~~the~~ EU-CyCLONe, ENISA shall, **with the support of ~~or~~ the CSIRTs network and with the approval ~~agreement~~ of the Member States concerned,** review and assess threats, **known exploitable** 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 **with the aim ~~to~~ of drawing lessons-learned to avoid or mitigate ~~a~~ future incident** to the **EU-CyCLONe, the** CSIRTs network, ~~the EU-CyCLONe~~ **the Member State concerned** 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,~~ **When an incident has an impact on a DEP-associated third country**, ~~the Commission~~ **ENISA** shall **also** share the report with **the Council**, ~~EU-CyCLONe, the CSIRT network, or and the Commission~~**. 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 **with** 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 ~~agreement~~ approval of 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, **known exploitable** vulnerabilities and lessons learned. It shall protect ~~**confidential**~~ information, **in particular** in accordance with Union or national law concerning the protection of sensitive or classified information. **If the Member State(s) or other user(s) concerned so requests, the report shall contain only anonymised data.**

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

5. **With the ~~agreement~~ approval of the Member State(s) concerned, ENISA may publish** ~~Wwhere possible,~~ a version of the report **containing only public information**. ~~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 **Cyber Hubs** and **Cross Border Cyber Hubs** ~~**[Cross-border SOCs collaboration 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 **deployable upon request in all Member States, Union institutions, bodies and agencies and in certain third countries''**;

(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[22] 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:

[22] 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).

‘(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 **way of** derogation **from** ~~**to**~~ Article 12(**14**~~**)**~~ 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.’;

(2a) Article 12 is amended as follows:

(1) paragraph 5 is replaced by the following:

5. The work programme may also provide that legal entities established in associated countries and legal entities that are established in the Union but are controlled from third countries are not eligible to participate in all or some actions under Specific Objective 3, for duly justified security reasons. In such cases, calls for proposals and calls for tenders shall be restricted to legal entities established or deemed to be established in Member States and controlled by Member States or by nationals of Member States.

The first subparagraph of this paragraph shall not apply, insofar as concerns legal entities that are established in the Union but are controlled ~~**form**~~ **from third countries, to any action implementing the European Cybersecurity Alert System** ~~**Reserve**~~ **where both of the following conditions are fulfilled in respect of that action:**

(a) there is a real risk, taking into account the results of the mapping referred to in Article 8 (3a) of Regulation [Cybersolidarity Act], that the tools, infrastructures and services necessary and sufficient for that action to adequately contribute to the objective of the European Cybersecurity Alert System will not be available ~~**that the technology, operational expertise or capacity necessary and sufficient for the EU Cybersecurity Reserve to adequately perform its functions will not be available in the**~~

~~Union~~ **from legal entities established or deemed to be established in Member States and controlled by Member States or by nationals of Member States; and**

(b) the security risk of procuring from such legal entities within the European Cybersecurity Alert System is proportionate to the benefits and does not undermine the essential security interests of the Union and its Member States. ~~including such legal entities within the EU Cybersecurity Reserve are proportionate to the benefits and do not undermine the essential security interests of the Union and its Member States.~~

The first subparagraph of this paragraph shall not apply, insofar as concerns legal entities that are established in the Union but are controlled from third countries, to actions implementing the EU Cybersecurity Reserve where both of the following conditions are fulfilled:

(a) there is a real risk,taking into account the results of the mapping referred to in Article 12 (7) of Regulation [Cybersolidarity Act], that the technology, expertise or capacity necessary and sufficient for the EU Cybersecurity Reserve to adequately perform its functions will not be available from legal entities established or deemed to be established in Member States and controlled by Member States or by nationals of Member States; and

(b) the security risk of including such legal entities within the EU Cybersecurity Reserve is proportionate to the benefits and does not undermine the essential security interests of the Union and its Member States.

(2) paragraph 6 is replaced by the following:

6. If duly justified for security reasons, the work programme may also provide that legal entities established in associated countries and legal entities that are established in the Union but are controlled from third countries may be eligible to participate in all or some actions under Specific Objectives 1 and 2, only if they comply with the requirements to be fulfilled by those legal entities to guarantee the protection of the essential security

interests of the Union and the Member States and to ensure the protection of classified documents information. Those requirements shall be set out in the work programme.

The first subparagraph of this paragraph shall also apply, insofar as concerns legal entities that are established in the Union but are controlled from third countries, to actions under Specific Objective 3:

(a) to implement the European Cybersecurity Alert System ~~Cybersecurity Reserve~~ in cases where paragraph 5, second subparagraph of this Article applies; and

(b) to implement the EU Cybersecurity Reserve in cases where paragraph 5, third subparagraph of this Article applies.'

(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.

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**~~ **selected Member States** 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. **The report shall in particular assess the effectiveness of the European Cyber Security Alert System, the Cyber Emergency Mechanism ~~as well as the effective~~ and the use of funding from DEP. It shall also assess how the regulation has contributed to reinforing solidarity and the competitive position of industry and services sectors in the Union across the digital economy as well as to the Union's technological sovereignty in the area of cybersecurity.**

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*

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 Cyber Hubs ~~SOCs~~ and Cross-border Cyber Hubs ~~SOCs~~ forming the European Cyber Alert System ~~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~~ ~~[…]~~