Council of the European Union
General Secretariat

Interinstitutional files:
2023/0109 (COD)

Brussels, 13 November 2023

WK 14873/2023 INIT

LIMITE

CYBER

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

WORKING DOCUMENT

From:	General Secretariat of the Council
To:	Horizontal Working Party on Cyber Issues
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 - Delegations' comments

Delegations will find in the Annex comments from the CZ, DK, DE, EE, IE, FR, HR, LV, HU, NL, AT, PL, FI and SE Delegations.

Contents

CZECH REPUBLIC

[…]

Whereas:

Commented [A1]: CZ did not have enough time to asses the recitals properly and does not see the point in doing so at this stage of the negotiations. First we have to find common ground and agreement on the text of the proposal itself, and only then we can adjust the recitals accordingly.

[…]

(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[1], it is necessary to increase the resilience of citizens, businesses and entities operating critical infrastructures against the growing cybersecurity threats, which can have devastating societal and economic impacts. Therefore, investment in infrastructures and services that will support faster detection and response to cybersecurity threats and incidents is needed, and Member States need assistance in better preparing for, as well as responding to significant and large-scale cybersecurity incidents. **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.

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

[…]

(7) It is necessary to strengthen the detection and situational awareness of cyber threats and incidents throughout the Union and to strengthen solidarity by enhancing Member States' and the Union's preparedness and capabilities to respond to significant and large-scale cybersecurity incidents. Therefore a pan-European infrastructure of SOCs (European Cyber**security** ~~Shield~~ ~~Alert~~ Support **System**) should be deployed 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**, with due respect for Member State competences and without duplication of the activities conducted by the CSIRT network, EU-CyCLONe and the NIS Cooperation Group**. These actions shall be without prejudice to Articles 107 and 108 of the Treaty on the Functioning of the European Union ('TFEU').

(8) To achieve these objectives, it is also necessary to amend Regulation (EU) 2021/694 of the European Parliament and of the Council[2] 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 DEP, which aims at guaranteeing the resilience, integrity and trustworthiness of the Digital Single Market, at strengthening capacities to monitor cyber-attacks and threats and to respond to them, and at reinforcing cross-border cooperation on cybersecurity. This will be complemented by the specific conditions under which financial support may be granted for those actions should be established and the governance and coordination mechanisms necessary in order to achieve the intended objectives should be defined. Other amendments to Regulation (EU) 2021/694 should include descriptions of proposed actions under the new operational objectives, as well as measurable indicators to monitor the implementation of these new operational objectives.

[…]

[2] 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).

(12) To more effectively prevent, assess and respond to cyber threats and incidents, it is necessary to develop more comprehensive knowledge about the threats to critical assets and infrastructures on the territory of the Union, including their geographical distribution, interconnection and potential effects in case of cyber-attacks affecting those infrastructures. A large-scale Union infrastructure of SOCs should be deployed ('the European Cyber**security** ~~Shield~~ **Alert System**'), comprising of several interoperating cross-border platforms, each grouping together several National SOCs. That infrastructure should serve national and Union cybersecurity interests and needs, leveraging state of the art technology for advanced data collection and analytics tools, enhancing cyber detection and management capabilities and providing real-time situational awareness. That infrastructure should serve to increase detection of cybersecurity threats and incidents and thus complement and support Union entities and networks responsible for crisis management in the Union, notably the EU Cyber Crises Liaison Organisation Network ('EU-CyCLONe'), as defined in Directive (EU) 2022/2555 of the European Parliament and of the Council[3].

(13) **Participation in the European ~~Cyber Shield~~ Cybersecurity ~~Alert~~ Support System should be voluntary for Member States.** Each Member State **that decides to join the European ~~Cyber Shield~~ Cybersecurity ~~Alert~~ Support System** should appoint the designated CSIRT under Directive 2022/2555 (NIS2), or another public body with a similar mandate, as defined in Article 2(2), that 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 cybersecurity threats and incidents and contributing to a Cross-border collaboration platform, as member of the cross-border collaboration platform ~~designate a **National SOC hub.** public body at national level tasked with coordinating cyber threat detection activities in that Member State.~~ ~~These National SOCs **hubs** should **have** act as **functionalities the capacity to act as** a reference point and gateway at national level for participation in the European Cyber Shield **Cybersecurity Alert System** and should **be**~~ **These entities should be** capable of detecting data ~~**, aggregating and analysing data**~~ **relevant to cyber threats and incidents, by using in particular state-of-the-art technologies and that would be shared appropriately with the CSIRT network in order to support the network conducting its activities. They should also ensure that cyber**

[3] 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).

threat information from public and private entities is shared and collected at national

Commented [A2]: This should be included in the text of the proposal, not the recital.

(14) As part of the European Cyber**security** ~~Alert~~ **Support System** ~~Shield~~, a number of Cross-border ~~Cybersecurity Operations Centres ('Cross-border SOCs')~~CTI collaboration platforms should be established. These should bring together National SOCs from at least three Member States, so that the benefits of cross-border threat detection and information sharing and management can be fully achieved. The general objective of Cross-border SOCs should be to strengthen capacities to analyse, prevent and detect cybersecurity threats and to support the production of high-quality intelligence on cybersecurity threats, notably through the sharing of **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.

(14a) A Member State selected by the European Cybersecurity Competence Centre (ECCC) following a call for expression of interest to set up a National SOC Hub or enhance the capabilities of an existing one, should jointly purchase relevant tools and infrastructures with the ECCC. Such a Member State should be eligible to receive a grant to operate the tools and infrastructures. 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 collaboration SOC Platform or enhance the capabilities of an existing one, should jointly purchase relevant tools and infrastructures with the ECCC. Such a Hosting Consortium should be eligible to receive a grant to operate the tools and infrastructures. 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 procurement procedure to purchase the relevant tools and infrastructures should be carried out jointly by the ECCC and relevant contracting authorities from the Member States selected following these calls for expressions of interest. Private entities should therefore not be eligible to participate in the calls for expression of interest to jointly purchase tools and infrastructures with the ECCC, or to receive grants to operate those tools and infrastructures. However, the Member States should have the possibility to involve private entities in the setting up, enhancement and operation of their National SOC Hubs and Cross-border SOCs Platforms in other ways which they deem appropriate, in compliance with national and Union law.

(15) At national level, the monitoring, detection and analysis of cyber threats is typically ensured by SOCs of public and private entities, in combination with CSIRTs. In addition, CSIRTs exchange information in the context of the CSIRT network, in accordance with Directive (EU) 2022/2555. The Cross-border SOCs should constitute a new capability that is complementary to the CSIRTs network **and will cooperate closely with it,** by pooling **data** and sharing **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.

[…]

(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**~~ cause**s** ~~**and impacts** of cybersecurity~~ **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 should be able to issue guidance in this respect.** This should make it possible to improve collective detection capacities and timely warnings to authorities and relevant entities, notably by using the latest artificial intelligence and data analytics technologies.

(20) By collecting, **correlating,** sharing and exchanging **data and information**, the European ~~Cyber Shield~~ **Cybersecurity Alert System** should enhance the Union's technological sovereignty. The pooling of high-quality curated data should also contribute to the development of advanced artificial intelligence and data analytics technologies. It should be facilitated through the connection of the European ~~Cyber Shield~~ **Cybersecurity Alert System** with the pan-European High Performance Computing infrastructure established by Council Regulation (EU) 2021/1173[4].

(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 'High Representative'), should gradually develop dedicated protocols and standards to allow for cooperation with the cyber defence community, including vetting and security conditions. The development of the European Cyber**security**

[4] 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).

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.

(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.

~~**(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 cybersecurity incidents and complement Member States' actions through emergency financial support for preparedness, response and **initial ~~immediate~~** recovery of essential services. That instrument should enable the rapid deployment of assistance in defined circumstances and under clear conditions and allow for a careful monitoring and evaluation of how resources have been used. Whilst the primary responsibility for preventing, preparing for and responding to cybersecurity incidents and crises lies with the Member States, the Cyber Emergency Mechanism promotes solidarity between Member States in accordance with Article 3(3) of the Treaty on European Union ('TEU').

(25) The Cyber Emergency Mechanism should provide support to Member States complementing their own measures and resources, and other existing support options in case of response to and **~~immediate~~ 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[5] **~~and Hybrid Rapid Response Teams~~**. It should address the need to ensure that specialised means are available to support preparedness and response to cybersecurity incidents across the Union and in third countries.

(26) This **~~instrument~~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~~**[6], **the EU Integrated Political Crisis Response Arrangements under Council Implementing Decision (EU) 2018/1993~~IPCR~~**[7] **(IPCR Arrangements),**

---

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

6 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).

7 **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.~~

Commission Recommendation 2017/1584[8] 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. 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 ENISA ~~the Commission~~ and the affected Member State should be ensured. When requesting support under the Cyber Emergency Mechanism, the Member State should provide relevant information justifying the need for support.

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

[8] **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).**

(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. For this purpose, the Commission, with the support of ENISA and in cooperation with the NIS Cooperation Group established by Directive (EU) 2022/2555, should regularly identify relevant sectors or subsectors, which should be eligible to receive financial support for coordinated testing at Union level. The sectors or subsectors should be selected from Annex I to Directive (EU) 2022/2555 ('Sectors of High Criticality'). The coordinated testing exercises should be based on common risk scenarios and methodologies. The selection of sectors and development of risk scenarios should take into account relevant Union-wide risk assessments and risk scenarios, including the need to avoid duplication, such as the risk evaluation and risk scenarios called for in the Council conclusions on the development of the European Union's cyber posture ~~to be~~ conducted by the Commission, the High Representative and the NIS Cooperation Group, in coordination with relevant civilian and military bodies and agencies and established networks, including the EU CyCLONe, as well as the risk assessment of communications networks and infrastructures requested by the Joint Ministerial Call of Nevers and conducted by the NIS Cooperation Group, with the support of the Commission and ENISA, and in cooperation with the Body of European Regulators for Electronic Communications (BEREC), the coordinated risk assessments to be conducted under Article 22 of Directive (EU) 2022/2555 and digital operational resilience testing as provided for in Regulation (EU) 2022/2554 of the European Parliament and of the Council[9]. 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**. 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

[9] 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

appropriate, it should complement the UCPM to ensure a comprehensive approach to respond to the impacts of cyber incidents on citizens.

[…]

(33) 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 or large-scale cybersecurity incidents. The EU Cybersecurity Reserve should ensure the availability and readiness of services. The services from the EU Cybersecurity Reserve should serve to support national authorities in providing assistance to affected entities operating in **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, Member States should specify the support provided to the affected entity at the national level, which should be taken into account when assessing the Member State request. ~~**The CSIRT Network established in Directive EU 2022/2555 can advise the Commission in 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.

Commented [A3]: This is not the role of the CNW and it should not be mandated in a recital.

(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, ENISA may be the contracting authority for those services with whose operation and administration it has been entrusted. The procurement procedures to establish the EU Cybersecurity Reserve should be conducted in accordance with Regulation EU 2018/1046. 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 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. 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 in 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 Cyber 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 NIS Cooperation Group, the Commission should ensure that the views of Member States as regards priorities and 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.

(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,** 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 relevant stakeholders, including representatives from the private sector, Member States, the Commission and other relevant EU institutions, bodies and agencies. As regards the private sector, ENISA is developing channels for exchanging information with specialised providers, including providers of managed security solutions

and vendors, in order to contribute to ENISA's mission of achieving a high common level of cybersecurity across the Union. Building on the collaboration with stakeholders, including the private sector, the review report on specific incidents should aim at assessing the causes, impacts and mitigations of an incident, after it has occurred. Particular attention should be paid to the input and lessons shared by the managed security service providers that fulfil the conditions of highest professional integrity, impartiality and requisite technical expertise as required by this Regulation. The report should be delivered and feed into the work of the EU~~=~~-CyCLONe, the CSIRTs network and the Commission. When the incident relates to a third country, it **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 as a whole. Therefore, third countries associated to the DEP may be supported from the EU Cybersecurity Reserve, where this is provided for in the ~~respective association~~ **relevant** agreement **or Association Council decision through which** ~~to~~ **the third country is associated** to DEP. **The CSIRT Network established in Directive EU 2022/2555 can advise the Commission in reviewing requests for support from the EU Cybersecurity Reserve.** 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~~.

Commented [A4]: This is not the role of the CNW, especially when it comes to third countries. Definitely should not be established in a recital.

(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.

[…]

HAVE ADOPTED THIS REGULATION:

Chapter I

GENERAL OBJECTIVES, SUBJECT MATTER, AND DEFINITIONS

Article 1

Subject-matter and objectives

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

   (a) the deployment of a pan-European infrastructure of Security Operations Centres ('European ~~Cyber Shield~~ **Cybersecurity Alert System**') to build and enhance common detection and situational awareness capabilities, with due respect of Member States' competences and complementary to activities conducted within the CSIRTs Network;

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

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

2. This Regulation pursues the objective to strengthen solidarity at Union level **and enhance Member States cyber resilience** through **the** following specific objectives:

   (a) to strengthen common Union detection and situational awareness of cyber threats and incidents thus allowing to reinforce the competitive position of industry and services sectors in the Union across the digital economy and contribute to the Union's technological sovereignty in the area of cybersecurity;

   (b) to reinforce preparedness of entities operating in **sectors of high** critical**ity** and ~~**highly**~~ **other** critical sectors across the Union and strengthen solidarity by developing **enhanced** ~~common~~ response capacities **to handle** ~~against~~ significant or large-scale cybersecurity incidents, including by making Union cybersecurity incident response

support available for third countries associated to the Digital Europe Programme ('DEP');

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

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

Commented [A5]: Wording in line with art. 4(2) TEU; "national security is Member States' sole responsibility." Strong point for CZ.

4. Without prejudice to Article 346 TFEU, the 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 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.

Article 2

Definitions

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

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

~~(a) it has the capacity to act as a reference point and gateway to other public and private organisations at national level for collecting and analysing information on cyber threats and incidents and contributing to a Cross-border SOC collaboration platform;~~

~~(b) its capability of detecting, aggregating and analysing relevant cyber threats and incidents by using in particular state of the art technologies;~~

(1) '**Cross-border** Cyber Threat Intelligence~~Security Operations Centre~~ **collaboration Platform' ("Cross-border** ~~SOC~~ CTI **collaboration Platform**") means a multi-country platform, **established by a written consortium agreeement** that brings together in a coordinated network structure N~~n~~ational ~~SOCs Hubs~~CSIRTs from at least three Member States ~~who form a Hosting Consortium~~, and that is designed to **monitor, detect and analyse** ~~prevent~~ cyber threats ~~and~~ **to prevent** incidents and to support the production of **cyber threat** ~~high-quality~~ intelligence, notably through the exchange of **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[10]; For the purpose of this Act, this is a public entity that has the following functionalities:

- it has the capacity to act as a reference point and gateway to other public and private organisations at national level for collecting and analysing information on cyber threats and incidents and contributing to a Cross-border CTI collaboration platform;
- it is capable of detecting, aggregating, and analysing data relevant to cyber threats and incidents by using in particular state of the art technologies;

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

(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;

Formatted: Font: (Default) +Headings CS (Times New Roman), Not Strikethrough

Formatted: Font: (Default) +Headings CS (Times New Roman), Not Strikethrough

Formatted: Font: (Default) +Headings CS (Times New Roman), Not Strikethrough

Formatted: Font: (Default) +Headings CS (Times New Roman), Not Strikethrough

Formatted: Bulleted + Level: 1 + Aligned at: 0.63 cm + Indent at: 1.27 cm

[10] 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).

(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;

(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;

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

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

~~(11)~~ **(8a) 'trusted providers'** means managed security service providers as defined in Article 6, point (40), of Directive (EU) 2022/2555 selected in accordance with Article 16 of this Regulation.

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

Chapter II

THE EUROPEAN ~~CYBER SHIELD~~ CYBERSECURITY ~~ALERT~~ SUPPORT SYSTEM

Article 3

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

1. An interconnected pan-European infrastructure **that consists** of **National SOC hubs and Cross-border ~~SOC~~ CTI collaboration platforms joining on a voluntary basis** ~~Security Operations Centres ('European Cyber Shield~~ **the European Cybersecurity ~~Alert~~ Support System**~~')~~ shall be established to **support the** develop**ment of** advanced capabilities for the Union to detect, analyse and process data on cyber threats and incidents in the Union. ~~It shall~~

~~consist of all National Security Operations Centres ('National SOCs') and Cross-border Security Operations Centres ('Cross-border SOCs').~~

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

2. The European ~~Cyber Shield~~ **Cybersecurity** Support~~Alert~~ **System** shall:

(a) pool analysed/aggregated **data** and share **information** ~~**data**~~ on cyber threats and incidents from various sources through cross-border ~~SOCs~~ CTI **collaboration platforms**;

(b) **share** ~~**produce**~~ high-quality, actionable information and cyber threat intelligence, through the use of state-of-the art tools **and advanced technologies such as**~~, notably~~ ~~**A**~~artificial ~~**I**~~intelligence 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, CSIRTs and the CSIRTs network**;

(d) contribute to **enhanced** ~~faster~~ detection of cyber threats and 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**~~ Support **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

Role of **National** CSIRTs ~~**Security Operations Centres**~~ ~~**Hubs**~~

Commented [A6]: To properly fulfill tasks and effectively achieve the objectives of the CSoA proposal, it is necessary to clearly differentiate between the tasks of the entities and mechanisms established within the CSoA and those set out in NIS 2. Only this will ensure an efficient, joint, non-duplicative and mutually supportive response to incidents and thus strengthen the common level of cybersecurity in the EU.

1. ~~In order~~ **Where a Member State decides** to **voluntarily** participate in the European ~~Cyber Shield~~ **Cybersecurity** ~~Alert~~ **Support System**, ~~each Member State~~ **it** shall designate ~~at least one~~a National ~~SOC Hub~~CSIRT pursuant to Directive (EU) 2022/2555 or another public body as defined in Article 2(2). ~~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~~ **Support System** ~~National SOCs~~ shall be selected by the European Cybersecurity Competence Centre ('ECCC') to **take part** ~~participate~~ in a joint procurement of tools and infrastructures with the ECCC**, in order to set up National SOC hubs or enhance capabilities of an existing one**. The ECCC may award grants to the selected **Member States** ~~National SOCs~~ to fund the operation of those tools and infrastructures. The Union financial contribution shall cover up to 50% of the acquisition costs of the tools and infrastructures, and up to 50% of the operation costs, with the remaining costs to be covered by the Member State. Before launching the procedure for the acquisition of the tools and infrastructures, the ECCC and the **Member State** ~~National SOC~~ shall conclude a hosting and usage agreement regulating the usage of the tools and infrastructures.

Commented [A7]: Suggest to move to a recital.

2a. In cases where the National CSIRT participating in the European Cybersecurity Alert System is not a member of the CSIRTs network, this entity shall ensure that it has procedural arrangements for information sharing with the respective Member State's CSIRTs network representative.

Commented [A8]: Strong point for CZ.

~~3. A **Member State** National SOC selected pursuant to paragraph 2 shall commit to apply **for their National SOC hubs** to participate in a Cross-border SOC **collaboration Platform** within two years from the date on which the tools and infrastructures are acquired, or on which it receives grant funding, whichever occurs sooner. If a **Member State's** National SOC **hub** is not a participant in a Cross-border SOC **collaboration Platform** by that time, **the Member State** it shall not be eligible for additional Union support under this **Chapter** Regulation.~~

Cross-border Cyber Threat Intelligence ~~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** ~~SOC hubs~~ **CSIRT or another public body, as defined in Article 2(2), work** ~~working~~ together to coordinate their cyber-detection and threat monitoring activities shall be eligible to participate in actions to establish a Cross-border ~~SOC~~ CTI **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 and infrastructures with the ECCC. The ECCC may award to the Hosting Consortium a grant to fund the operation of the tools and infrastructures. The Union financial contribution shall cover up to 75% of the acquisition costs of the tools and infrastructures, and up to 50% of the operation costs, with the remaining costs to be covered by the Hosting Consortium. Before launching the procedure for the acquisition of the tools and infrastructures, the ECCC and the Hosting Consortium shall conclude a hosting and usage agreement regulating the usage of the tools and infrastructures.

Commented [A9]: Preference to move this part to a recital

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~~agreement.

4. A Cross-border ~~SOC~~ CTI **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 ~~SOC~~ CTI 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 and infrastructures already jointly procured with that Hosting Consortium.

Article 6

Cooperation and information sharing within and between cross-border ~~SOCs~~ CTI collaboration Platforms

1. Having established the cross-border CTI platform, Members of a Hosting Consortium shall **ensure ~~that their National SOC hubs~~relevant information** exchange among themselves within the Cross-border CTI collaboration Platform**, in accordance with the Consortium Agreement,** ~~relevant information among themselves within the 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:

   […]

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

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

   (b) a governance framework **clarifying and** incentivising the sharing of information **referred to in paragraph 1** by all participants;

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

3. To encourage exchange of information between Cross-border ~~SOCs~~ CTI **collaboration Platforms**, Cross-border ~~SOCs~~ CTI **collaboration Platforms** shall ensure a high level of interoperability between themselves. ~~To facilitate the interoperability between the Cross-border SOCs collaboration Platforms, the Commission may, by means of implementing acts, after consulting the ECCC, specify the conditions for this interoperability. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2) of this Regulation. Before submitting those draft implementing acts to the committee referred to in Article 21(1), the Commission shall consult the ECCC and existing Cross-border SOC collaboration Platforms.~~

   Commented [A10]: Strong point for CZ to delete this part.

4. Cross-border ~~SOCs~~ CTI **collaboration 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. 1. Where the Cross-border ~~SOCs~~ CTI **collaboration Platforms** obtain information relating to a potential or ongoing large-scale cybersecurity incident, ~~they~~ it shall **ensure** ~~provide~~ **that** ~~data from the CSIRTs~~ in accordance with the principles for managing large-scale cybersecurity incidents in Directive (EU) 2022/2555 and their standard operating procedures, the CSIRTs networks will notify and share this information with EU-CyCLONe if relevant.

2. Each cross-border CTI collaboration platform shall ensure that it has procedural arrangements for the information sharing in paragraph 1.

3. Cross-border CTI collaboration platforms shall, where appropriate, ensure that experiences with state of the art tools, notably Artificial Intelligence and data analytics technology, used within the cross-border CTI collaboration platforms, are shared with the CSIRTs Network.

Commented [A11]: Strong point for CZ.

Security

1. Member States participating in the European ~~Cyber Shield~~ **Cybersecurity** ~~Alert~~ **Support System** shall ensure a high level of data security and physical security of the European ~~Cyber Shield~~ **Cybersecurity** ~~Alert~~ **Support 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~~ **Support System** shall ensure that the sharing of information within the European ~~Cyber Shield~~ **Cybersecurity** ~~Alert~~ **Support 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.

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** paragraph**s** 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.

Chapter III

CYBER EMERGENCY MECHANISM

Article 9

Establishment of the Cyber Emergency Mechanism

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

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

Article 10

Type of actions

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

   (a) preparedness actions**:**~~, including~~

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

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

   (b) ~~response~~ actions~~,~~ supporting response to and **initiating** ~~immediate~~ recovery from significant and large-scale cybersecurity incidents, to be provided by trusted providers participating in the EU Cybersecurity Reserve established under Article 12;

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

Commented [A13]: The funds that have not been used in the Reserve ex post should be used for preparedness ex ante in order to efficiently use the funds. One idea could be to set aside a certain amount of money for ex post activiteies every year, and move the leftovers to the next year's funds for ex ante activities of the Reserve.

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

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

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

2. The definition of the process associated to the coordinated preparedness testing shall be the sole competence of the Member States.

2. The NIS Cooperation Group in cooperation with the Commission, ENISA, and the High Representative, shall develop common risk scenarios and methodologies for the **coordinated testing exercises under Article 10 (1) (a) (i). The NIS Cooperation Group, in cooperation with Commission, ENISA and the High Representative, may develop common risk scenarios and methodologies for other preparedness actions under Article 10(1)(a)(ii).**

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, responding or providing support for responding to significant or large-scale cybersecurity incidents, and ~~immediate~~ **initiate** recovery from such incidents.

2. The EU Cybersecurity Reserve shall consist of incident response services from trusted providers selected in accordance with the criteria laid down in Article 16. The Reserve shall

Commented [A14]: Overall, CZ believes that there is still a lot of question marks regarding the practical functionalities of the Reserve which require broader and more elaborate discussions. Moreover, all processes regarding its functioning need to be specified in the text of the proposal, so that we all have a common understanding of the working of the Reserve.

include pre-committed services. The ~~services~~ **Reserve shall** be deployable **upon request** in all Member States **and in third countries referred to in Article 17 (1).**

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

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

   (b) CERT-EU, on behalf of Union institutions, bodies and agencies.

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

4. Users referred to in paragraph 3, point (a), shall use the services **granted upon their request** from the EU Cybersecurity Reserve in order to respond or support response to and **initiate** ~~immediate~~ recovery from significant or large-scale incidents affecting entities operating in **sectors of high** critical**ity** or ~~**highly**~~ **other** critical sectors, if assessed as beneficial by the user.

5. ~~The Commission~~ENISA shall responsibility **have overall responsibility** for the implementation of the EU Cybersecurity Reserve. **To that end, ~~the Commission~~ENISA, in cooperation with the NIS Cooperation Group ~~and ENISA~~,** shall determine the priorities and evolution of the EU Cybersecurity Reserve, in line with the requirements of the users referred to in paragraph 3 ,.The ECCC ~~and~~ shall ~~supervise~~ monitor the~~its~~ implementation, and ensure complementarity, consistency, synergies and links with other support actions under this Regulation as well as other Union actions and programmes, pursuant to the ECCC's strategic tasks as outlined in article 5 of EU 2021/887. **These priorities shall be revised every two years.**

6. In order to fulfil its obligations under this regulation and in order not to compromise existing obligations of the Agency under other Union law, the adequate staffing and financing of ENISA shall be ensured.

~~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.~~

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). **Before submitting those drafting implementing acts to the committee referred to in Article 21(1), the Commission may exchange advice and cooperate with the NIS Cooperation Group.**~~

Commented [A15]: We still question the need of prepaid services.

Commented [A16]: There is a lot of information on how the deployment works on request of Member States, but there is no information included on how processes would work for EUIBAs. Following the logic for Member States, it should be CERT-EU requesting assistance on behalf of an EUIBA, when CERT-EU couldn't handle an incident alone. Throughout the text **full allignment is needed with the EUIBAs regulation** and it should be spelled out how the mechanisms would apply and work for EUIBAs.

Formatted: Font: (Default) +Headings CS (Times New Roman), Not Bold, No underline

Commented [A17]: Despite the current change, there is no guarantee the tasks given fall solely under ENISA authority.

Commented [A18]: Needs specification in the text, not later by the means of implementing acts.

Article 13

Requests for support from the EU Cybersecurity Reserve

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

2. To receive support from the EU Cybersecurity Reserve, the users referred to in Article 12(3) shall exhaust all other ~~take **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 from users referred to in Article 12(3), point (a), of this Regulation shall be transmitted to ~~the Commission and~~ ENISA via the Single Point of Contact designated or established by the Member State in accordance with Article 8(3) of Directive (EU) 2022/2555.

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

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

   (a) appropriate information on how the provisions of article 9 and 10 of Directive (EU) 2022/2555 have been met as regard~~ing~~ the affected entity and potential impacts of the incident **on affected Member State(s) and users, including the risk of spill over,** and the planned use of the requested support, including an indication of the estimated needs;

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

   (c) **where relevant, available** information about other forms of support available to the affected entity~~, including contractual arrangements in place for incident response and **initial** immediate recovery services, as well as insurance contracts potentially covering such type of incident.~~

5a. The information provided in accordance with paragraph 5 of this Article shall be handled in accordance with Union law while preserving the security and commercial interests of the entity concerned. ENISA shall handle this information with utmost cautionsness and not disclose it to any other parties.

~~7. The Commission may, by means of implementing acts, specify the detailed arrangements for allocating the EU Cybersecurity Reserve support services that implement the tasks provided for in Article 12(1) and in accordance with the allocation criteria provided for in Article 12(3).~~

Commented [A19]: Should already be specified within this regulation. Strong point for CZ.

Implementation of the support from the EU Cybersecurity Reserve

1. Requests for support from the EU Cybersecurity Reserve, shall be assessed by ~~the Commission, with the support of~~ ENISA ~~or as defined in contribution agreements under Article 12(6)~~, and a ~~response~~ decision shall be transmitted to the users referred to in Article 12(3) without delay **and in any event no later than 72 hours from the submission of the request to ensure effectiveness of the support action**.

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

   […]

   (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 and then Union institutions, bodies and agencies.

2a. The decision to provide EU Cybersecurity Reserve services shall be taken by the Council.

Commented [A20]: We suggest to include the following in a recital:

Given the situation in which the EU Cybersecurity Reserve would be deployed, the role of the Council during the times of crisis remains crucial. Therefore, the deployment of the EU Cybersecurity Reserve shall be decided by the Council, given its role under the EU Integrated Political Crisis Response Arrangements. In cases of deployment to third countries as defined in article 17 of this regulation, the decision shall be taken by the Council, in cooperation with the High Representative.

Formatted: Font: (Default) +Headings CS (Times New Roman), Not Bold, No underline

3. The EU Cybersecurity Reserve services shall be provided in accordance with specific agreements between the service provider and the user to which the support under the EU Cybersecurity Reserve is provided. Those agreements shall include liability conditions. Before procuring services for the EU Cybersecurity Reserve, the contracting authority and the provider shall conclude a liability agreement. This agreement shall exclude the liability of the contracting authority regarding the deployment of the provider.

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~~ 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.

6. Within **three** ~~one~~ month**s** from the end of the support action, the users shall provide **the** Commission**,** ~~and~~ ENISA**, the CSIRTs network and, where appropiate, EU-CyCLONe** with a summary report about the service provided, results achieved and the lessons learned. When the user is from a third country as set out in Article 17, such report shall be shared with the High Representative and the Council.

7. The Commission shall report to the NIS Cooperation Group**, on a regular basis and at least once per year,** about the use and the results of the support~~, on a regular basis~~.

~~*Article 15*~~

~~**Coordination with crisis management mechanisms**~~

~~1. In cases where significant or large-scale cybersecurity incidents originate from or result in disasters as defined in Decision 1313/2013/EU[11], the support under this Regulation for responding to such incidents shall complementactions under and without prejudice to Decision 1313/2013/EU.~~

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

~~3. In consultation with the High Representative, support under the Cyber Emergency Mechanism may complement assistance provided in the context of the Common Foreign and Security Policy and Common Security and Defence Policy, including through the Cyber Rapid Response Teams. It may also complement or contribute to assistance provided by one Member State to another Member State in the context of Article 42(7) of the Treaty on the European Union.~~

~~4. Support under the Cyber Emergency Mechanism may form part of the joint response between the Union and Member States in situations referred to in Article 222 of the Treaty on the Functioning of the European Union.~~

Article 16

Trusted providers

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

   (a) ensure **that the services included in** the EU Cybersecurity Reserve **are such that the Reserve** ~~includes services that~~ may be deployed in all Member States, taking into

[11] 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).

account in particular national requirements for the provision of such services, including certification or accreditation;

[…]

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

[…]

(d) the provider shall have appropriate security clearance, at least for personnel intended for service deployment**~~:~~ ,where required by a Member State;**

[…]

(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.

Article 17

Support to DEP-associated third countries

1. **A DEP- associated t~~T~~**hird countr**~~y~~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 shall be 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.

[…]

5. **In order to enable the ~~Commission~~ ENISA to apply the criteria listed in Article 14(2) to requests from third countries referred to in paragraph 1, p~~P~~**rior to receiving any support from the EU Cybersecurity Reserve, third countries shall provide to the ~~Commission~~ ENISA **~~and the High Representative~~** and the High Representative ~~-~~information about their cyber resilience and risk management capabilities, including at least information on national measures taken to prepare for significant or large-scale cybersecurity incidents, as well as information on responsible national entities, including CSIRTs or equivalent entities, their capabilities and the resources allocated to them. **~~The Commission~~** ENISA **shall share this information with the High Representative, for the purpose of facilitating the cooperation referred to in paragraph 6**. Where provisions of Articles 13 and 14 of this Regulation refer to Member States, they shall apply to third countries as set out in paragraph 1.

6. The ~~Commission~~ ENISA shall **inform the** Council ~~NIS Cooperation Group~~ **~~Council~~** and **cooperate** ~~coordinate~~ with the High Representative about the requests received and the implementation of the support granted to third countries from the EU Cybersecurity Reserve ~~The Commission shall ensure that the NIS Cooperation Group and the High Representative are provided~~

Commented [A21]: Not clear why this change has been made. Council needs to be informed as it should be the one making the decisions about providing EU Cybersecurity Reserve. (see art. 14, 2a).

Commented [A22]: Deployment will be decided by Council so it is ensured that its opinion has already been taken into account.

Article 17a) ~~15~~

Coordination with Union crisis management mechanisms

1. **~~In cases w~~Where a significant cybersecurity incident or a large-scale cybersecurity incident~~s~~ originate~~s~~ from or result~~s~~ in a disaster~~s~~ as defined in Article 4, point (1), of Decision No 1313/2013/EU[12], 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~~, 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.**

~~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~~

~~12 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).~~

~~**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 A**~~at the request of the Commission, the EU-CyCLONe or the CSIRTs network, **and with the agreement of the Member States concerned,** ENISA shall review and assess threats, vulnerabilities and mitigation actions with respect to a specific significant or large-scale cybersecurity incident. Following the completion of a review and assessment of an incident, ENISA shall deliver an incident review report to the CSIRTs network, the EU-CyCLONe and the Commission to support them in carrying out their tasks, in particular in view of those set out in Articles 15 and 16 of Directive (EU) 2022/2555. ~~**Where relevant,**~~ **When an incident has an impact on a third country**, the Commission shall share the report with the High Representative.

2. To prepare the incident review report referred to in paragraph 1, ENISA shall collaborate all relevant stakeholders, including representatives of Member States, the Commission, other relevant EU institutions, bodies and agencies, managed security services providers and users of cybersecurity services. Where appropriate, **and ~~in close cooperation~~ with the agreement 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, 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) 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 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~~ **Support System**, including the development, deployment and operation of National and ~~Cross-border SOCs~~CTI **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';

(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[13] with the exception of actions implementing the EU Cybersecurity Reserve, which shall be implemented by the Commission and ENISA.**';**

[…]

(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.

[…]

Article 20

Evaluation

By [~~four~~ two 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.

[13] 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).

[…]

DENMARK

[…]

Whereas:

[…]

(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[14], it is necessary to increase the resilience of citizens, businesses and entities operating critical infrastructures against the growing cybersecurity threats, which can have devastating societal and economic impacts. Therefore, investment in infrastructures and services that will support faster detection and response to cybersecurity threats and incidents is needed, and Member States need assistance in better preparing for, as well as responding to significant and large-scale cybersecurity incidents. **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.

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

[…]

(7) It is necessary to strengthen the detection and situational awareness of cyber threats and incidents throughout the Union and to strengthen solidarity by enhancing Member States' and the Union's preparedness and capabilities to respond to significant and large-scale cybersecurity incidents. Therefore a pan-European infrastructure of SOCs (European Cyber**security** ~~Shield~~ **Alert System**) should be deployed 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**, with due respect for Member State competences and without duplication of the activities conducted by the CSIRT network, EU-CyCLONe and the NIS Cooperation Group**. These actions shall be without prejudice to Articles 107 and 108 of the Treaty on the Functioning of the European Union ('TFEU').

(8) To achieve these objectives, it is also necessary to amend Regulation (EU) 2021/694 of the European Parliament and of the Council[15] 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 DEP, which aims at guaranteeing the resilience, integrity and trustworthiness of the Digital Single Market, at strengthening capacities to monitor cyber-attacks and threats and to respond to them, and at reinforcing cross-border cooperation on cybersecurity. This will be complemented by the specific conditions under which financial support may be granted for those actions should be established and the governance and coordination mechanisms necessary in order to achieve the intended objectives should be defined. Other amendments to Regulation (EU) 2021/694 should include descriptions of proposed actions under the new operational objectives, as well as measurable indicators to monitor the implementation of these new operational objectives.

[…]

(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

---

15 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).

infrastructures on the territory of the Union, including their geographical distribution, interconnection and potential effects in case of cyber-attacks affecting those infrastructures. A large-scale Union infrastructure of SOCs should be deployed ('the European Cyber**security** ~~Shield~~ **Alert System**'), comprising of several interoperating cross-border platforms, each grouping together several National SOC Hubs. That infrastructure should serve national and Union cybersecurity interests and needs, leveraging state of the art technology for advanced data collection and analytics tools, enhancing cyber detection and management capabilities and providing real-time situational awareness. That infrastructure should serve to increase detection of cybersecurity threats and incidents and thus complement and support Union entities and networks responsible for crisis management in the Union, notably the EU Cyber Crises Liaison Organisation Network ('EU-CyCLONe'), as defined in Directive (EU) 2022/2555 of the European Parliament and of the Council[16].

(13) **Participation in ~~the~~a cross-border SOC collaboration platform and the ~~European Cyber Shield~~ Cybersecurity Alert System ~~is~~should be voluntary for Member States.** Each Member State **that decides to join ~~the European Cyber Shield Cybersecurity Alert System~~a cross-border SOC collaboration platform** should designate a **National SOC hub.** ~~public body at national level tasked with coordinating cyber threat detection activities in that Member State.~~ These National SOC~~s~~ **hubs** should **have** ~~act~~ as **functionalities the capacity to act as** a reference point and gateway at national level for participation in the European ~~Cyber Shield~~ **Cybersecurity Alert System** and should **be capable of detecting, aggregating and analysing data relevant to cyber threats and incidents, by using in particular state-of-the-art technologies and that would be shared appropriately with the CSIRT network in order to support the network 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 or existing national platforms 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.**

Commented [A23]: The term National SOC Hubs should be used throughout the document to avoid confusion.

Commented [A24]: 'Should be' is replaced with 'is' to underline that participation is voluntary.

Commented [A25]: For clarification purposes 'European Cyber Shield Cyber Security Alert System' is replaced with 'a cross-border SOC collaboration platform', since the former is not what the member states are primarily signing up to participate in (the MS are signing up to take part in a cross-border SOC collaboration platform). As it stands now, the wording changes the focus of the cooperation from the regional to the EU level (where we already have existing collaboration in the form of the CSIRT- network).

Commented [A26]: Building state-of-the-art situational awareness and detection capabilities demands an active exchange of information between public and private actors. However, our national experience tells us that attracting companies into CERT collaborations requires putting in place very clear guarantees that the companies have tight control with their shared information.

We find it difficult to cultivate the public-private-partnerships needed to advance the creation of cutting-edge European CTI as long as private entities must enter into a collaboration, where they will lose control over the sharing of their information, which risks having substantial commercial and financial repercussions.

[16] 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).

(14) As part of the European Cyber**security Alert System** ~~Shield~~, a number of Cross-border Cybersecurity Operations Centres ('Cross-border SOCs') should be established. These should bring together National SOC Hubs from at least three Member States, so that the benefits of cross-border threat detection and information sharing and management can be fully achieved. The general objective of Cross-border SOCs should be to strengthen capacities to analyse, prevent and detect cybersecurity threats and to support the production of high-quality intelligence on cybersecurity threats, notably through the sharing of **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.

(14a) A Member State selected by the European Cybersecurity Competence Centre (ECCC) following a call for expression of interest to set up a National SOC Hub or enhance the capabilities of an existing one, should jointly purchase relevant tools and infrastructures with the ECCC. Such a Member State should be eligible to receive a grant to operate the tools and infrastructures. 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 collaboration SOC Platform or enhance the capabilities of an existing one, should jointly purchase relevant tools and infrastructures with the ECCC. Such a Hosting Consortium should be eligible to receive a grant to operate the tools and infrastructures. 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 procurement procedure to purchase the relevant tools and infrastructures should be carried out jointly by the ECCC and relevant contracting authorities from the Member States selected following these calls for expressions of interest. Private entities should therefore not be eligible to participate in the calls for expression of interest to jointly purchase tools and infrastructures with the ECCC, or to receive grants to operate those tools and infrastructures. However, the Member States should have the possibility to involve private entities in the setting up, enhancement and operation of their National SOC Hubs and Cross-border SOCs Platforms in other ways which they deem appropriate, in compliance with national and Union law.

(15) At national level, the monitoring, detection and analysis of cyber threats is typically ensured by SOCs of public and private entities, in combination with CSIRTs. In addition, CSIRTs exchange information in the context of the CSIRT network, in accordance with Directive (EU) 2022/2555. The Cross-border SOCs should constitute a new capability that is complementary to the CSIRTs network **and will cooperate closely with it,** by pooling **data** and sharing **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.

[…]

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

Commented [A27]: OBS PÅ CFCS KOMMENTAR HER. I relation til artikel 7.

(18) Entities participating in a cross-border SOC collaboration platform ~~the European Cybersecurity 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~~ cause**s** ~~and impacts of cybersecurity~~ **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 a cross-border SOC collaboration platform ~~the European Cybersecurity Alert System~~ ~~Shield~~ should be equipped with state-of-the-art and highly-secure tools, equipment and infrastructures. **The Commission should be able to issue guidance in this respect.** This should make it possible to improve collective detection capacities and timely warnings to authorities and relevant entities, notably by using the latest artificial intelligence and data analytics technologies.

(20) By collecting, **correlating,** sharing and exchanging **data and information**, the European ~~Cyber Shield~~ **Cybersecurity Alert System** should enhance the Union's technological sovereignty. The pooling of high-quality curated data should also contribute to the development of advanced artificial intelligence and data analytics technologies. It should be facilitated through the connection of the European ~~Cyber Shield~~ **Cybersecurity Alert System** with the pan-European High Performance Computing infrastructure established by Council Regulation (EU) 2021/1173[17].

[17] 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).

(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 'High Representative'), should gradually develop dedicated protocols and standards to allow for cooperation with the cyber defence community, including vetting and security conditions. The development of the European Cyber**security 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.

(22) Information sharing among participants of a cross-border SOC collaboration platform and 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.

~~**(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 cybersecurity incidents and complement Member States' actions through emergency financial support for preparedness, response and **initial ~~immediate~~** recovery of essential services. That instrument should enable the rapid deployment of assistance in defined circumstances and under clear conditions and allow for a careful monitoring and evaluation of how resources have been used. Whilst the primary responsibility for preventing, preparing for and responding to cybersecurity incidents and crises lies with the Member States, the Cyber Emergency Mechanism promotes solidarity between Member States in accordance with Article 3(3) of the Treaty on European Union ('TEU').

(25) The Cyber Emergency Mechanism should provide support to Member States complementing their own measures and resources, and other existing support options in case of response to and **~~immediate~~ 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[18] **~~and Hybrid Rapid Response Teams~~**. It should address the need to ensure that specialised means are available to support preparedness and response to cybersecurity incidents across the Union and in third countries.

Commented [A28]: The reference to article 42 (7) implies that provisions under CYSOL should be able to respond to attacks that could potentially be above the threshold of an armed attack and thus activate the solidarity clause in 42 (7). Such incidents would be dealt with inside the scope of the CFSP and would be a part of the MS preogative on national security and defence, and should not be subject to, nor included in regulation under TFEU.

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

(26) This ~~instrument~~**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~~[19], **the EU Integrated Political Crisis Response Arrangements under Council Implementing Decision (EU) 2018/1993**~~IPCR~~[20] **(IPCR Arrangements), Commission Recommendation 2017/1584**[21] 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. 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.

[…]

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

---

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

20 **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.~~

21 **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).**

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 functioning of essential services.

(29) As part of the preparedness actions, to promote a consistent approach and strengthen security across the Union and its internal market, support should be provided for testing and assessing cybersecurity of entities operating in ~~**highly critical**~~ sectors **of high criticality** identified pursuant to Directive (EU) 2022/2555 in a coordinated manner. For this purpose, the Commission, with the support of ENISA and in cooperation with the NIS Cooperation Group established by Directive (EU) 2022/2555, should regularly identify relevant sectors or subsectors, which should be eligible to receive financial support for coordinated testing at Union level. The sectors or subsectors should be selected from Annex I to Directive (EU) 2022/2555 ('Sectors of High Criticality'). The coordinated testing exercises should be based on common risk scenarios and methodologies. The selection of sectors and development of risk scenarios should take into account relevant Union-wide risk assessments and risk scenarios, including the need to avoid duplication, such as the risk evaluation and risk scenarios called for in the Council conclusions on the development of the European Union's cyber posture ~~to be~~ conducted by the Commission, the High Representative and the NIS Cooperation Group, in coordination with relevant civilian and military bodies and agencies and established networks, including the EU CyCLONe, as well as the risk assessment of communications networks and infrastructures requested by the Joint Ministerial Call of Nevers and conducted by the NIS Cooperation Group, with the support of the Commission and ENISA, and in cooperation with the Body of European Regulators for Electronic Communications (BEREC), the coordinated risk assessments to be conducted under Article 22 of Directive (EU) 2022/2555 and digital operational resilience testing as provided for in Regulation (EU) 2022/2554 of the European Parliament and of the Council[22]. 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

[22] 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

entities operating in ~~highly critical~~ sectors **of high criticality**. 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.

[…]

(33) 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 or large-scale cybersecurity incidents. The EU Cybersecurity Reserve should ensure the availability and readiness of services. The services from the EU Cybersecurity Reserve should serve to support national authorities in providing assistance to affected entities operating in **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, Member States should specify the support provided to the affected entity at the national level, which should be taken into account when assessing the Member State request. **The CSIRT Network established in Directive EU 2022/2555 can advise the Commission in 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.

(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, ENISA may be the contracting authority for those services with whose operation and administration it has been entrusted. The procurement procedures to establish the EU Cybersecurity Reserve should be conducted in accordance with Regulation EU 2018/1046. 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 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. 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 in 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 Cyber 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 NIS Cooperation Group, the Commission should ensure that the views of Member States as regards priorities and 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.

(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**~~,~~ **and with the agreement 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

Commented [A29]: Insertion made in order for the language in the preamble to match the language in article 18 and to emphasize that a review process cannot be initiated without explicit approval of the affected MS.

significant or large-scale cybersecurity incident. After the completion of a review and assessment of an incident, ENISA should prepare an incident review report, in collaboration with relevant stakeholders, including representatives from the private sector, Member States, the Commission and other relevant EU institutions, bodies and agencies. As regards the private sector, ENISA is developing channels for exchanging information with specialised providers, including providers of managed security solutions and vendors, in order to contribute to ENISA's mission of achieving a high common level of cybersecurity across the Union. Building on the collaboration with stakeholders, including the private sector, the review report on specific incidents should aim at assessing the causes, impacts and mitigations of an incident, after it has occurred. Particular attention should be paid to the input and lessons shared by the managed security service providers that fulfil the conditions of highest professional integrity, impartiality and requisite technical expertise as required by this Regulation. The report should be delivered and feed into the work of the EU~~=~~-CyCLONe, the CSIRTs network and the Commission. When the incident relates to a third country, it **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 as a whole. Therefore, third countries associated to the DEP may be supported from the EU Cybersecurity Reserve, where this is provided for in the ~~respective association~~ **relevant** agreement **or Association Council decision through which ~~to~~ the third country is associated** to DEP. **The CSIRT Network established in Directive EU 2022/2555 can advise the Commission in reviewing requests for support from the EU Cybersecurity Reserve.** 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~~.

(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.

[…]

HAVE ADOPTED THIS REGULATION:

Chapter I

GENERAL OBJECTIVES, SUBJECT MATTER, AND DEFINITIONS

Article 1

Subject-matter and objectives

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

   (a) the deployment of a pan-European infrastructure of Security Operations Centres ('European ~~Cyber Shield~~ **Cybersecurity Alert System**') to build and enhance common detection and situational awareness capabilities with due respect of Member States competences and complementary to activities conducted within the CSIRT network;

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

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

2. This Regulation pursues the objective to strengthen solidarity at Union level **and enhance Member States cyber resilience** through **the** following specific objectives:

   […]

   (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 capacities **to handle** ~~against~~ significant or large-scale

cybersecurity incidents, including by making Union cybersecurity incident response support available for third countries associated to the Digital Europe Programme ('DEP');

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

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

~~4.~~ The obligations laid down in this Regulation shall not entail the supply of information the disclosure of which would be contrary to the essential interests of Member States' national security, public security or defence.

~~5~~4. Without prejudice to Article 346 TFEU, the 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 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.

Article 2

Definitions

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

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

(a) it has the capacity to act as a reference point and gateway to other public and private organisations at national level for collecting and analysing ~~information~~ on cyber threats and incidents and contributing to a Cross-border SOC collaboration platform;

Commented [A30]: Insertion is made in order to underline the voluntary nature of this initiative. Also 'directly- and indirectly' is inserted, since large-scale incidents typically have a cross-border nature, and thus, what happens in one MS can have ramifications for other MS (i.e. telecom companies that are affected may operate in many MS simultaneously)

Commented [A31]: Insertion made in order to streamline the text with TEU art. 4 (2).

Formatted: Point Manual

Commented [A32]: Insertion made with respect to TEU art. 4 (2). Sharing of information which would be against the national security interests of MS should not be subject to this Regulation. This also relates to pp 38(a) and art. 7.

Commented [A33]: The sharing of confidential information is not supposed to happen within Cyber Security Alert System (at the most, sensitive information should be shared within this system).

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

(1) '**Cross-border Security Operations Centre collaboration Platform' ("Cross-border SOC collaboration Platform**") means a multi-country platform, **established by a written consortium agreeement** that brings together in a coordinated network structure **N~~n~~**ational SOC**~~s~~ Hubs** from at least three Member States ~~who form a Hosting Consortium~~, and that is designed to **monitor, detect and analyse** ~~prevent~~ cyber threats ~~and~~ **to prevent** incidents and to support the production of **cyber threat** ~~high-quality~~ intelligence, notably through the exchange of **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[23];~~

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

(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;

Commented [A34]: 'State of the art technologies' should be defined in the subsequent parts of this article, seeing that so much emphasis is put on said concept in the current compromise proposal.

Commented [A35]: Changes made in order to secure that it is the national SOC hubs that are the members of the hosting consortium.

[23] 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).

(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;

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

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

~~(11)~~ **(8a)** **'trusted providers'** means managed security service providers as defined in Article 6, point (40), of Directive (EU) 2022/2555 selected in accordance with Article 16 of this Regulation.

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

Chapter II

THE EUROPEAN ~~CYBER SHIELD~~ CYBERSECURITY ALERT SYSTEM

Article 3

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

1. A~~n interconnected~~ pan-European infrastructure **that consists** of **National SOC hubs and Cross-border SOC collaboration platforms joining on a voluntary basis** ~~Security Operations Centres ('European Cyber Shield~~ **the European Cybersecurity Alert System**~~')~~ shall be established to **support the** develop**ment of** advanced capabilities for the Union to detect, analyse and process data on cyber threats and incidents in the Union. ~~It shall consist of all National Security Operations Centres ('National SOCs') and Cross-border Security Operations Centres ('Cross-border SOCs').~~

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

2. The European ~~Cyber Shield~~ **Cybersecurity Alert System** shall:

Commented [A36]: It is unclear what is meant by interconnected here. The National SOC hubs that will be directly interconnected, are those entering into a consortium.

Could be relevant to create a new recital, which carves out what is meant by interconnected.

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

(b) **share** ~~**produce**~~ high-quality, actionable information ~~and cyber threat intelligence~~, through the use of state-of-the art tools **and advanced technologies such as**~~, notably~~ ~~**A**~~**a**rtificial ~~**I**~~**i**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, CSIRTs and the CSIRTs network**;

(d) contribute to **enhanced** ~~faster~~ detection of cyber threats and 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 Security Operations Centres~~s~~ 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 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.~~

Commented [A37]: DK proposes to delete the reference to CTI, seeing that the CTI acquired in a cross-border SOC collaboration platform might be subject to commercial restrictions set by the provider, from which it is bought, and thus, cannot necessarily be shard at the EU level.

Furthermore, if the CTI is to be shared at the EU level, this might impose extra costs on the consortiums, since the provider hereof most likely will raise the prices, if the CTI are to be shared with more member states.

2. Following a call for expression of interest, **Member States intending to participate in a cross-border SOC collaboration platform** ~~**the European Cyber Shield Cybersecurity Alert System** National SOCs~~ shall be selected by the European Cybersecurity Competence Centre ('ECCC') to **take part** ~~participate~~ in a joint procurement of tools and infrastructures with the ECCC**, in order to set up National SOC hubs or enhance capabilities of an existing one**. The ECCC may award grants to the selected **Member States** ~~National SOCs~~ to fund the operation of those tools and infrastructures. The Union financial contribution shall cover up to 50% of the acquisition costs of the tools and infrastructures, and up to 50% of the operation costs, with the remaining costs to be covered by the Member State. Before launching the procedure for the acquisition of the tools and infrastructures, the ECCC and the **Member State** ~~National SOC~~ shall conclude a hosting and usage agreement regulating the usage of the tools and infrastructures.

3. A **Member State** ~~National SOC~~ selected pursuant to paragraph 2 shall commit to apply **for their National SOC hubs** to participate in a Cross-border SOC **collaboration Platform** within two years from the date on which the tools and infrastructures are acquired, or on which it receives grant funding, whichever occurs sooner. If a **Member State's** National SOC **hub** is not a participant in a Cross-border SOC **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 Security Operations Centres~~-~~ collaboration Platforms

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

[…]

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~~agreement.

4. A 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~~

Commented [A38]: European Cyber Shield Cyber Security Alert System' is deleted, since this is not what the member states are primarily signing up to participate in (MS are signing up to take part in a cross-border SOC collaboration platform).

Commented [A39]: We find that this condition goes beyond the initial call for interest, and infringes upon the voluntary nature of participating in the European Cybersecurity Alert System.

Commented [A40]: Changes made in order to secure that it is the national SOC hubs that are the members of the hosting consortium.

~~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 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 and infrastructures already jointly procured with that Hosting Consortium.

Commented [A41]: Denmark is positive towards this inclusion in the text.

Article 6

Cooperation and information sharing within and between cross-border SOCs~~s~~ collaboration Platforms

1. Members of a Hosting Consortium shall **ensure that their National SOC hubs** voluntarily exchange**, in accordance with the Consortium Agreement,** relevant information ~~among themselves~~ within the 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:

Commented [A42]: Deleted for semantical reasons.

Commented [A43]: The type of information to be shared among members of the cross-border SOC platforms is to be decided upon in the Consortium arrangements. As COM has confirmed that this is a list of examples, we believe it should be deleted.

Why has only parts of the paragraph been deleted?

[…]

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

   (a) a commitment to share **among the members of the Consortium** on a voluntary basis ~~a significant amount of data~~ **information** referred to in paragraph 1, and the conditions under which that information is to be exchanged;

   (b) a governance framework **clarifying and** incentivising the sharing of information **referred to in paragraph 1** by all participants;

Commented [A44]: Building these platforms means building sufficient trust between participants to share information. There is a need to maintain sufficient leaway for participants to make the collaboration in the platforms effective.

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

3. ~~To encourage exchange of information between Cross-border SOCs **collaboration Platforms**, Cross-border SOCs **collaboration Platforms** shall ensure a high level of interoperability between themselves. To facilitate the interoperability between the Cross-border SOCs **collaboration Platforms**, the Commission may, by means of implementing acts**, after consulting the ECCC,** specify the conditions for this interoperability. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2) of this Regulation. **Before submitting those draft implementing acts to the committee referred to in Article 21(1), the Commission shall consult the ECCC and existing Cross-border SOC collaboration Platforms.**~~

Article 7

Cooperation and information sharing with Union-level entities and networks

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

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

3. Cross-border SOC platforms shall, where appropriate, ensure that experiences with state of the art tools, notably Artificial Intelligence and data analytics technology, used within the cross-border SOC platforms is shared with the CSIRTs Network.

Article 8

Security

1. Member States participating in the European ~~Cyber Shield~~ **Cybersecurity Alert System** shall ensure a high level of data security and physical security of the European ~~Cyber Shield~~ **Cybersecurity Alert System** infrastructure, and shall ensure that the infrastructure ~~shall be~~ **is**

Commented [A46]: Denmark awaits debate on this article at the HWPCI meeting november 13 before we are able to provide written comments and textual compromises to this article.

Denmarks needs confirmation from the Commission on the fact that "procedural arrangments" in para 2 entails how information is to be shared, but not what is shared and when it is shared.

Commented [A47]:

Commented [A48]: To show that the experiences of the Cross-border platforms will benefit the CSIRTs network.

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 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.

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** paragraph**s** 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.

Commented [A49]: Denmark is positive towards this compromise, which we find to be moving in the right direction.

Chapter III

CYBER EMERGENCY MECHANISM

Article 9

Establishment of the Cyber Emergency Mechanism

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

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

Article 10

Type of actions

1. The Mechanism, consisting of a fund from where user referred to in Article 12 (3) on a voluntary basis can request assistance, shall support the following types of actions:

(a) preparedness actions**:**~~,~~ ~~including~~

(iii) the coordinated preparedness testing of entities operating in **sectors of high criticality** ~~highly critical sectors~~ across the Union;

(iv) other preparedness actions for entities operating in sectors of high criticality ~~**critical**~~ **and other** ~~**highly**~~ **critical sectors, including those involving exercises and trainings and ;**

(b) ~~response~~ actions~~,~~ supporting response to and **initiating** ~~immediate~~ recovery from significant and large-scale cybersecurity incidents, to be provided by trusted providers participating in the EU Cybersecurity Reserve established under Article 12;

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

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

Article 11

Voluntary Coordinated preparedness testing of entities

1. For the purpose of supporting the coordinated preparedness testing of entities referred to in Article 10(1), point (a), across the Union, **and with due respect to the** ~~**Member States**~~ **competences of all directly and indirectly involved Member States,** the Commission, after consulting the NIS Cooperation Group and ENISA, shall identify the sectors, or sub-sectors, concerned, from the Sectors of High Criticality listed in Annex I to Directive (EU) 2022/2555 from which **Member States may request to participate and to this end propose** entities to ~~may~~ be subject to the coordinated preparedness testing.~~,~~

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

Commented [A50]: The insertion is made order to emphazise the voluntary nature of this initative, as confirmed by COM in the preliminary discussions on CYSOL in HWPCI.

COM confirmed in a preliminary HWPCI discussion that the "Mechanism" is a fund.

Commented [A51]: We find this compromise to move in the right direction. However, we still believe it should be deleted in order to highlight the voluntary nature of the initiative.

Commented [A52]: The insertion is made order to emphazise the voluntary nature of this initative, as confirmed by COM in the preliminary discussions on CYSOL.

Commented [A53]: Insertion made in order to take into account a scenario, where the preparedness testing involves entities that operate in more than one member state.

Commented [A54]: DK assumes that if the preparedness testing involves entities, which operate in more than one member state, then all affected MS will have to agree hereto, not only the one receiving the funding. We kindly request the Presidency to reach out COM in order to receive their confirmation on this. If this is not the case, then a reservation should be built into the article, in order for it to clearly state that any transnational preparedness testing requires the explicit approval from all MS directly and indirectly involved.

We have not received confirmation regarding this as of yet. Thus the reservation still stands.

2. The NIS Cooperation Group in cooperation with the Commission, ENISA, and the High Representative, shall develop common risk scenarios and methodologies for the **coordinated testing exercises under Article 10 (1) (a) (i). The NIS Cooperation Group, in cooperation with Commission, ENISA and the High Representative, may develop common risk scenarios and methodologies for other preparedness actions under Article 10(1)(a)(ii).**

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, responding or providing support for responding to significant or large-scale cybersecurity incidents, and ~~immediate~~ **initiate** recovery from such incidents.

2. The EU Cybersecurity Reserve shall consist of incident response services from trusted providers selected in accordance with the criteria laid down in Article 16. The Reserve shall include pre-committed services. The ~~services~~ **Reserve shall** be deployable **upon request** in all Member States **and in third countries referred to in Article 17 (1).**

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

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

   (b) ~~Union institutions, bodies and agencies.~~CERT EU

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

Commented [A55]: Should be the same proces for EUIBAS as for MS.

4. Users referred to in paragraph 3, point (a), shall use the services **granted upon their request** from the EU Cybersecurity Reserve in order to respond or support response to and **initiate** ~~immediate~~ recovery from significant or large-scale incidents affecting entities operating in **sectors of high** critical**ity** or ~~**highly**~~ **other** critical sectors.

5. The Commission shall responsibility **have overall responsibility** for the implementation of the EU Cybersecurity Reserve. **To that end, the** Commission**, in cooperation with the NIS Cooperation Group and ENISA,** shall determine the priorities and evolution of the EU Cybersecurity Reserve, in line with the requirements of the users referred to in paragraph 3, and shall supervise its implementation, and ensure complementarity, consistency, synergies and links with other support actions under this Regulation as well as other Union actions and programmes. **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 a mapping of the services needed **and their availability**, after consulting ~~**Member States**~~ **the NIS Cooperation Group** and the Commission. ENISA shall prepare a similar mapping, after consulting the **the NIS Cooperation Group and the** Commission, to identify the needs of third countries eligible for support from the EU Cybersecurity Reserve pursuant to Article 17. The Commission, where relevant, **may** ~~shall~~ **seek the views of** ~~**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). **Before submitting those drafting implementing acts to the committee referred to in Article 21(1), the Commission may exchange advice and cooperate with the NIS Cooperation Group.**

Article 13

Requests for support from the EU Cybersecurity Reserve

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

2. To receive support from the EU Cybersecurity Reserve, the users referred to in Article 12(3) shall take ~~appropriate~~ **exhaust all other** 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.

Commented [A56]: To align with the Commission's explanation that the Cyber Reserve would be the an additional service, once all national measures have been exhausted.

[…]

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

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

(a) appropriate information regarding the affected entity and potential impacts of the incident **on affected Member State(s) and users, including the risk of spill over,** and the planned use of the requested support, including an indication of the estimated needs;

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

(c) **where relevant, available** information about other forms of support available to the affected entity, including contractual arrangements in place for incident response and **initial** ~~immediate~~ recovery services, as well as insurance contracts potentially covering such type of incident.

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

[…]

Article 14

Implementation of the support from the EU Cybersecurity Reserve

1. Requests for support from the EU Cybersecurity Reserve, shall be assessed by the Commission, with the support of ENISA or as defined in contribution agreements under Article 12(6), and a response shall be transmitted to the users referred to in Article 12(3) without delay **and in any event no later than 72 hours from the submission of the request to ensure effectiveness of the support action**.

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

[…]

(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 and Union institutions, bodies and agencies.

2a. The decision to provide EU Cybersecurity Reserve services shall be approved by the Council.

[…]

Commented [A57]: Deploying the reserve to a third country is a matter of foreign and security policy, which is a Council prerogative. Moreover, if the reserve is sent during a conflict, it could raise questions of international law.

Any deployment of the reserve must be approved by the Council.

6. Within **three** ~~one~~ month**s** from the end of the support action, the users shall provide **t**he Commission**,** ~~and~~ ENISA**, the CSIRTs network and, where appropiate, EU-CyCLONe** with a summary report about the service provided, results achieved and the lessons learned. When the user is from a third country as set out in Article 17, such report shall be shared with the High Representative.

7. The Commission shall report to the NIS Cooperation Group**, on a regular basis and at least once per year,** about the use and the results of the support~~, on a regular basis~~.

~~*Article 15*~~

~~**Coordination with crisis management mechanisms**~~

~~1. In cases where significant or large-scale cybersecurity incidents originate from or result in disasters as defined in Decision 1313/2013/EU[24], the support under this Regulation for responding to such incidents shall complementactions under and without prejudice to Decision 1313/2013/EU.~~

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

~~3. In consultation with the High Representative, support under the Cyber Emergency Mechanism may complement assistance provided in the context of the Common Foreign and Security Policy and Common Security and Defence Policy, including through the Cyber Rapid Response Teams. It may also complement or contribute to assistance provided by one Member State to another Member State in the context of Article 42(7) of the Treaty on the European Union.~~

~~4. Support under the Cyber Emergency Mechanism may form part of the joint response between the Union and Member States in situations referred to in Article 222 of the Treaty on the Functioning of the European Union.~~

Article 16

Trusted providers

~~[24]~~ Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism (OJ L 347, 20.12.2013, p. 924).

1. 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** combined **services included in** the EU Cybersecurity Reserve **are such that the Reserve** ~~includes services that~~ may be deployed in all Member States, taking into account in particular national requirements for the provision of such services, including certification or accreditation;

   […]

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

   […]

   (d) the provider shall have appropriate security clearance, at least for personnel intended for service deployment**~~:~~,where required by a Member State;**

   […]

   (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.

Commented [A58]: This remains unclear to us.

It needs to be stated who will provide this security clearance. Will a security clearance from a state outside the EU be sufficient ? Will MS be able to deny the use of a provider if they do not have a security clearance from that Member State ?

Article 17

Support to DEP-associated third countries

1. **A DEP- associated t**~~**T**~~hird countr**y**~~**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 shall be 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.

[…]

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, p~~P~~**rior to receiving any support from the EU Cybersecurity Reserve, third countries shall provide to the Commission **~~and the High Representative~~** information about their cyber resilience and risk management capabilities, including at least information on national measures taken to prepare for significant or large-scale cybersecurity incidents, as well as information on responsible national entities, including CSIRTs or equivalent entities, their capabilities and the resources allocated to them. **The Commission shall share this information with the High Representative, for the purpose of facilitating the cooperation referred to in paragraph 6**. Where provisions of Articles 13 and 14 of this Regulation refer to Member States, they shall apply to third countries as set out in paragraph 1.

6. The Commission shall **inform the NIS Cooperation Group ~~Council~~ and cooperate~~coordinate~~** with the High Representative about the requests received and the implementation of the support granted to third countries from the EU Cybersecurity Reserve. **The Commission shall take into account the opinions of the NIS Cooperation Group and the High Representative, if such are provided.**

Commented [A59]: We fail to understand wh ythe NISCG is mentioned here, as the NISCG does not play a role in common foreign and security policy.

This is insufficient. Deploying the reserve to a third country is a matter of foreign and security policy, which is a Council prerogative. Moreover, if the reserve is sent during a conflict, it could raise questions of international law.

Any deployment of the reserve must be approved by the Council.

Article 17a) ~~15~~

Coordination with Union crisis management mechanisms

1. **~~In cases w~~Where a significant cybersecurity incident or a large-scale cybersecurity incident~~s~~ originate~~s~~ from or result~~s~~ in a disaster~~s~~ as defined in Article 4, point (1), of Decision No 1313/2013/EU[25], 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~~, 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**

[25] ~~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).~~

Regulation for responding to such incident shall be handled in accordance with the relevant ~~protocols and~~ procedures under the IPCR Arrangements.

~~**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 A**~~at the request of the Commission, the EU-CyCLONe or the CSIRTs network, **and with the agreement of the Member States concerned,** ENISA shall review and assess threats, vulnerabilities and mitigation actions with respect to a specific significant or large-scale cybersecurity incident. Following the completion of a review and assessment of an incident, ENISA shall deliver an incident review report to the CSIRTs network, the EU-CyCLONe and the Commission to support them in carrying out their tasks, in particular in view of those set out in Articles 15 and 16 of Directive (EU) 2022/2555. ~~**Where relevant,**~~ **When an incident has an impact on a third country**, the Commission shall share the report with the High Representative.

2. To prepare the incident review report referred to in paragraph 1, ENISA shall collaborate all relevant stakeholders, including representatives of Member States, the Commission, other relevant EU institutions, bodies and agencies, managed security services providers and users of cybersecurity services. Where appropriate, **and ~~in close cooperation~~ with the agreement 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~~

Commented [A60]: We do not see the added value of this article, as ENISA is already capable of conducting such reports, and does so within the CSIRT-network.

Thus, we would prefer to delete the article.

If the article is to remain, it must be crystal clear, that ENISA cannot conduct such reviews without the explicit consent and approval of the member states concerned.

It should be clear that ENISA cannot collaborate with entities in a Member State without the explicit approval of the Member State – preferably their national CSIRT og national cyber crisis management authority.

~~consult other types of stakeholders.~~ Consulted representatives shall disclose any potential conflict of interest.

3. The report shall cover a review and analysis of the specific significant or large-scale cybersecurity incident, including the main causes, vulnerabilities and lessons learned. It shall protect **~~confidential~~** information, **in particular** in accordance with Union or national law concerning the protection of sensitive or classified information. **If the Member State(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 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 and Cross-border SOC~~s~~ **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';

(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[26] with the exception of actions implementing the EU Cybersecurity Reserve, which shall be implemented by the Commission and ENISA.**';**

[…]

(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.

[…]

[26] 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).

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

Article 20

Evaluation

By [~~four~~ two 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 focus on the effective use of funding from DEP how the regulation has contributed to reinforing 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 as well as the effectiveness of the Cyber Emergency Mechanism.

Commented [A61]: The review should be conducted after two years, so that any Lessons learned can be incorporated before the next MFF starts.

Formatted: Font: (Default) +Headings CS (Times New Roman), Not Bold

Commented [A62]: It should be more specified what the review should focus on.

Would like for COM/ES chairmanship to elaborate on why this has not been included in the compromise.

[…]

GERMANY

[…]

Whereas:

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

(2) The magnitude, frequency and impact of cybersecurity incidents are increasing, including supply chain attacks aiming at cyberespionage, ransomware or disruption. They represent a major threat to the functioning of network and information systems. In view of the fast- evolving threat landscape, the threat of possible large-scale incidents causing significant disruption or damage to critical infrastructures demands heightened preparedness at all levels of the Union's cybersecurity framework. That threat goes beyond Russia's military aggression on Ukraine, and is likely to persist given the multiplicity of state-aligned, criminal and hacktivist actors involved in current geopolitical tensions. Such incidents can impede the provision of public services and the pursuit of economic activities, including in **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[1], it is necessary to increase the resilience of citizens, businesses and entities operating critical infrastructures against the growing cybersecurity threats, which can have devastating societal and economic impacts. Therefore, investment in infrastructures and services that will support faster detection and response to

cybersecurity threats and incidents is needed, and Member States need assistance in better preparing for, as well as responding to significant and large-scale cybersecurity incidents. **Building on the existing structures and in close cooperation with them,** ~~T~~the Union should also increase its capacities in these areas, notably as regards the collection and analysis of data on cybersecurity threats and incidents.

(4) The Union has already taken a number of measures to reduce vulnerabilities and increase the resilience of critical infrastructures and entities against cybersecurity risks, in particular Directive (EU) 2022/2555 of the European Parliament and of the Council[1], Commission Recommendation (EU) 2017/1584[2], Directive 2013/40/EU of the European Parliament and of the Council[3] and Regulation (EU) 2019/881 of the European Parliament and of the Council[4]. In addition, the Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure invites Member States to take urgent and effective measures, and to cooperate loyally, efficiently, in solidarity and in a coordinated manner with each other, the Commission and other relevant public authorities as well as the entities concerned, to enhance the resilience of critical infrastructure used to provide essential services in the internal market.

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

---

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

2 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).

3 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).

4 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).

5 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[1] 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 cybersecurity incidents. Therefore a pan-European infrastructure of SOCs (European Cyber**security** ~~Shield~~ **Alert System**) should be deployed 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**, with due respect for Member State competences and without duplication of the activities conducted by the CSIRT network, EU-CyCLONe and the NIS Cooperation Group**. These actions shall be without prejudice to Articles 107 and 108 of the Treaty on the Functioning of the European Union ('TFEU').

Commented [AS63]: This is a good change.

1 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[1] in certain areas. In particular, this Regulation should amend Regulation (EU) 2021/694 as regards adding new operational objectives related to the European Cyber**security** ~~Shield~~ **Alert System** and the Cyber Emergency Mechanism under Specific Objective 3 of DEP, which aims at guaranteeing the resilience, integrity and trustworthiness of the Digital Single Market, at strengthening capacities to monitor cyber-attacks and threats and to respond to them, and at reinforcing cross-border cooperation on cybersecurity. This will be complemented by the specific conditions under which financial support may be granted for those actions should be established and the governance and coordination mechanisms necessary in order to achieve the intended objectives should be defined. Other amendments to Regulation (EU) 2021/694 should include descriptions of proposed actions under the new operational objectives, as well as measurable indicators to monitor the implementation of these new operational objectives.

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

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

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

(11) For the purpose of sound financial management, specific rules should be laid down for the carry-over of unused commitment and payment appropriations. While respecting the principle that the Union budget is set annually, this Regulation should, on account of the unpredictable, exceptional and specific nature of the cybersecurity landscape, provide for possibilities to carry over unused funds beyond those set out in the Financial Regulation, thus maximising the Cybersecurity Emergency Mechanism's capacity to support Member States in countering effectively cyber threats.

(12) To more effectively prevent, assess and respond to cyber threats and incidents, it is necessary to develop more comprehensive knowledge about the threats to critical assets and infrastructures on the territory of the Union, including their geographical distribution, interconnection and potential effects in case of cyber-attacks affecting those infrastructures. A large-scale Union infrastructure of SOCs should be deployed ('the European Cyber**security** ~~Shield~~ **Alert System**'), comprising of several interoperating cross-border platforms, each grouping together several National SOCs. That infrastructure should serve national and Union cybersecurity interests and needs, leveraging state of the art technology for advanced data collection and analytics tools, enhancing cyber detection and management capabilities and providing real-time situational awareness. That infrastructure should serve to increase detection of cybersecurity threats and incidents and thus complement and support Union entities and networks responsible for crisis management in the Union, notably the EU Cyber Crises Liaison Organisation Network ('EU-CyCLONe'), as defined in Directive (EU) 2022/2555 of the European Parliament and of the Council[1].

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

(13) **Participation in the European ~~Cyber Shield~~ Cybersecurity ~~Alert~~ Supporting System should be voluntary for Member States.** Each Member State **that decides to join the European ~~Cyber Shield~~ Cybersecurity Alert System** should designate a **National SOC hub.** ~~public body at national level tasked with coordinating cyber threat detection activities in that Member State.~~ These National SOC~~s~~ **hubs** should **have** ~~act~~ as **functionalities the capacity to act as** a reference point and gateway at national level for participation in the European ~~Cyber Shield~~ **Cybersecurity Alert System** and should **be capable of detecting, aggregating and analysing data relevant to cyber threats and incidents, by using in particular state-of-the-art technologies and that would be shared appropriately with the CSIRT network in order to support the network 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 or existing national platforms 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~~ Supporting System** ~~Shield~~, a number of Cross-border Cybersecurity Operations Centres ('Cross-border SOCs') should be established. These should bring together National SOCs from at least three Member States, so that the benefits of cross-border threat detection and information sharing and management can be fully achieved. The general objective of Cross-border SOCs should be to strengthen capacities to analyse, prevent and detect cybersecurity threats and to support the production of high- quality intelligence on cybersecurity threats, notably through the sharing of **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.

Commented [AS64]: Ok…Do you have suggestions regarding this point? It would be crucial to understand from the beginning how tasks will be divided and how they will complement each other. This is totally unclear and if remains so, it will undermine the functioning of these infrastructures. We proposed some changes in Art. 6

Commented [RS65]: We asked for deletion/point was not taken up → Justification: This cannot be a task of the SOC hubs since it is a task to be decided by every MS in his own responsibility taking into account those provisions laid down by NIS2.

Commented [RS66]: The term "cybersecurity alert system" is not ideal since it creates a high expectation for the outside world. In a situation where not all MS are participating in this activity (since it is voluntary) this term may lead to misunderstandings. A better name could be "CS supporting system"

(14a) A Member State selected by the European Cybersecurity Competence Centre (ECCC) following a call for expression of interest to set up a National SOC Hub or enhance the capabilities of an existing one, should jointly purchase relevant tools and infrastructures with the ECCC. Such a Member State should be eligible to receive a grant to operate the tools and infrastructures. 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 collaboration SOC Platform or enhance the capabilities of an existing one, should jointly purchase relevant tools and infrastructures with the ECCC. Such a Hosting Consortium should be eligible to receive a grant to operate the tools and infrastructures. 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 procurement procedure to purchase the relevant tools and infrastructures should be carried out jointly by the ECCC and relevant contracting authorities from the Member States selected following these calls for expressions of interest. Private entities should therefore not be eligible to participate in the calls for expression of interest to jointly purchase tools and infrastructures with the ECCC, or to receive grants to operate those tools and infrastructures. However, the Member States should have the possibility to involve private entities in the setting up, enhancement and operation of their National SOC Hubs and Cross-border SOCs Platforms in other ways which they deem appropriate, in compliance with national and Union law.

(15) At national level, the monitoring, detection and analysis of cyber threats is typically ensured by SOCs of public and private entities, in combination with CSIRTs. In addition, CSIRTs exchange information in the context of the CSIRT network, in accordance with Directive (EU) 2022/2555. The Cross-border SOCs should constitute a new capability that is complementary to the CSIRTs network **and will cooperate closely with it,** by pooling **data** and sharing **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 SOCs should act as a central point allowing for a broad pooling of relevant data and cyber threat intelligence, enable the spreading of threat information among a large and diverse set of actors (e.g., Computer Emergency Response Teams ('CERTs'), CSIRTs, Information Sharing and Analysis Centers ('ISACs'), operators of critical infrastructures). The information exchanged among participants in a Cross-border SOC could include data from networks and sensors, threat intelligence feeds, indicators of compromise, and contextualised information about incidents, threats and vulnerabilities. In addition, Cross-border SOCs should also enter into cooperation agreements with other Cross-border SOCs.

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

(18) Entities participating in the European Cyber**security** ~~Alert~~ **Supporting 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~~ cause**s** ~~and impacts~~ ~~of cybersecurity~~ **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~~ **Supporting System** ~~Shield~~ should be equipped with state-of-the-art and highly-secure tools, equipment and infrastructures. **The Commission should be able to issue guidance in this respect.** This should make it possible to improve collective detection capacities and timely warnings to authorities and relevant entities, notably by using the latest artificial intelligence and data analytics technologies.

(20) By collecting, **correlating,** sharing and exchanging **data and information**, the European ~~Cyber Shield~~ **Cybersecurity** ~~Alert~~ **Supporting System** should enhance the Union's technological sovereignty. The pooling of high-quality curated data should also contribute to the development of advanced artificial intelligence and data analytics technologies. It should be facilitated through the connection of the European ~~Cyber Shield~~ **Cybersecurity** ~~Alert~~ **Supporting System** with the pan-European High Performance Computing infrastructure established by Council Regulation (EU) 2021/1173[1].

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

(21) While the European Cyber**security** ~~Alert~~ **Supporting 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 'High Representative'), should gradually develop dedicated protocols and standards to allow for cooperation with the cyber defence community, including vetting and security conditions. The development of the European Cyber**security** ~~Alert~~ **Supporting 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.

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

(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 cybersecurity incidents and complement Member States' actions through emergency financial support for preparedness, response and **initial ~~immediate~~** recovery of essential services. That instrument should enable the rapid deployment of assistance in defined circumstances and under clear conditions and allow for a careful monitoring and evaluation of how resources have been used. Whilst the primary responsibility for preventing, preparing for and responding to cybersecurity incidents and crises lies with the Member States, the Cyber Emergency Mechanism promotes solidarity between Member States in accordance with Article 3(3) of the Treaty on European Union ('TEU').

(25) The Cyber Emergency Mechanism should provide support to Member States complementing their own measures and resources, and other existing support options in case of response to and **~~immediate~~ 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[1] **~~and Hybrid Rapid Response Teams~~**. It should address the need to ensure that specialised means are available to support preparedness and response to cybersecurity incidents across the Union and in third countries.

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

(26) This ~~instrument~~**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~~[1], **the EU Integrated Political Crisis Response Arrangements under Council Implementing Decision (EU) 2018/1993**~~IPCR~~[2] **(IPCR Arrangements)**, ~~**Commission Recommendation 2017/1584**~~[3] 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. 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 should be ensured. When requesting support under the Cyber Emergency Mechanism, the Member State should provide relevant information justifying the need for support.

---

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

2 **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.~~

~~3~~ ~~**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).**~~

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

(29) As part of the preparedness actions, to promote a consistent approach and strengthen security across the Union and its internal market, support should be provided for testing and assessing cybersecurity of entities operating in ~~**highly critical**~~ sectors **of high criticality** identified pursuant to Directive (EU) 2022/2555 in a coordinated manner. For this purpose, the Commission, with the support of ENISA and in cooperation with the NIS Cooperation Group established by Directive (EU) 2022/2555, should regularly identify relevant sectors or subsectors, which should be eligible to receive financial support for coordinated testing at Union level. The sectors or subsectors should be selected from Annex I to Directive (EU) 2022/2555 ('Sectors of High Criticality'). The coordinated testing exercises should be based on common risk scenarios and methodologies. The selection of sectors and development of risk scenarios should take into account relevant Union-wide risk assessments and risk scenarios, including the need to avoid duplication, such as the risk evaluation and risk scenarios called for in the Council conclusions on the development of the European Union's cyber posture ~~to be~~ conducted by the Commission, the High Representative and the NIS Cooperation Group, in coordination with relevant civilian and military bodies and agencies and established networks, including the EU CyCLONe, as well as the risk assessment of communications networks and infrastructures requested by the Joint Ministerial Call of Nevers and conducted by the NIS Cooperation Group, with the support of the Commission

and ENISA, and in cooperation with the Body of European Regulators for Electronic Communications (BEREC), the coordinated risk assessments to be conducted under Article 22 of Directive (EU) 2022/2555 and digital operational resilience testing as provided for in Regulation (EU) 2022/2554 of the European Parliament and of the Council[1]. The selection of sectors should also take into account the Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure.

(30) In addition, the Cyber Emergency Mechanism should offer support for other preparedness actions and support preparedness in other sectors, not covered by the coordinated testing of entities operating in **~~highly critical~~** sectors **of high criticality**. 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 assistance provided by Member States to a Member State affected by a significant or large-scale cybersecurity incident, including by the CSIRTs network set out in Article 15 of Directive (EU) 2022/2555. Member States providing assistance should be allowed to submit requests to cover costs related to dispatching of expert teams in the framework of mutual assistance. The eligible costs could include travel, accommodation and daily allowance expenses of cybersecurity experts.

(33) A Union-level Cybersecurity Reserve should gradually be set up, consisting of services from **trusted** private providers of managed security services to support response and **~~immediate~~ initiate** recovery actions in cases of significant or large-scale cybersecurity incidents. The EU Cybersecurity Reserve should ensure the availability and readiness of services. The services from the EU Cybersecurity Reserve should serve to support national authorities in providing assistance to affected entities operating in **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, Member States should specify the

---

1 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December

2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011

support provided to the affected entity at the national level, which should be taken into account when assessing the Member State request. **The CSIRT Network established in Directive EU 2022/2555 can advise the Commission in 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.

Commented [AS67]: We propose a different approach in Art. 12.
Only in case of a "crisis" situation there should be a review by COM/CSIRTs NW.

(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, ENISA may be the contracting authority for those services with whose operation and administration it has been entrusted. The procurement procedures to establish the EU Cybersecurity Reserve should be conducted in accordance with Regulation EU 2018/1046. 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 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. 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~~can be deployed quickly in case of a request for support from the EU Cybersecurity Reserve, direct contact between the applicant and the potential provider should be provided ~~, they may be based on templates prepared by ENISA, after consulting Member States.~~**

Commented [RS68]: Please refer to our proposal in Art. 12

(33b) **Due regard should be given to the role of the Member States in 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 Cyber 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 NIS Cooperation Group, the Commission should ensure that the views of Member States as regards priorities and 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.

(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,** 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 relevant stakeholders, including representatives from the private sector, Member States, the Commission and other relevant EU institutions, bodies and agencies. As regards the private sector, ENISA is developing channels for exchanging information with specialised providers, including providers of managed security solutions and vendors, in order to contribute to ENISA's mission of achieving a high common level of cybersecurity across the Union. Building on the collaboration with stakeholders, including the private sector, the review report on specific incidents should aim at assessing the causes, impacts and mitigations of an incident, after it has occurred. Particular attention should be paid to the input and lessons shared by the managed security service providers that fulfil the conditions of highest professional integrity, impartiality and requisite technical expertise as required by this Regulation. The report should be delivered and feed into the work of the EU=-CyCLONe, the CSIRTs network and the Commission. When the incident relates to a third country, it **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 as a whole. Therefore, third countries associated to the DEP may be supported from the EU Cybersecurity Reserve, where this is provided for in the ~~respective association~~ **relevant** agreement **or Association Council decision through which ~~to~~ the third country is associated** to DEP. **The CSIRT Network established in Directive EU 2022/2555 can advise the Commission in reviewing requests for support from the EU Cybersecurity Reserve in case of a crisis/IPCR activation.** 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**~~.

(38) In order to ensure uniform conditions for the implementation of this Regulation, ~~implementing powers should be conferred on~~ the Commission **may prepare ~~some~~ guidance ~~material~~documents** to ~~specify the~~outline 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.

Commented [RS69]: Red line: no implementing powers w.r.t. interoperability requs and info sharing in case of large scale incidents

The COM should not decide on procedural arrangement for information sharing when it comes to large scale incidents. Overall, this should be national responsibility and a responsibility for those institutions/networks which are already established such as CyCLONe (acc. to NIS2).

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

HAVE ADOPTED THIS REGULATION:

Chapter I

GENERAL OBJECTIVES, SUBJECT MATTER, AND DEFINITIONS

Article 1

Subject-matter and objectives

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

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

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

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

2. This Regulation pursues the objective to strengthen solidarity at Union level **and enhance Member States cyber resilience** through **the** following specific objectives:

   (a) to strengthen common Union detection and situational awareness of cyber threats and incidents thus allowing to reinforce the competitive position of industry and services sectors in the Union across the digital economy and contribute to the Union's technological sovereignty in the area of cybersecurity;

   (b) to reinforce preparedness of entities operating in **sectors of high** critical**ity** and ~~**highly**~~ **other** critical sectors across the Union and strengthen solidarity by developing **enhanced** ~~common~~ response capacities **to handle** ~~against~~ significant or large-scale

cybersecurity incidents, **building upon those provisions established through Directive (EU) 2022/2555,** including by making Union cybersecurity incident response

support available for third countries associated to the Digital Europe Programme ('DEP');

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

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

4. Without prejudice to Article 346 TFEU, the 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. In case information is exchanged ~~T~~the exchange of such information 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.

Commented [RS70]: In general, there are few to none possibilities for condfidential exchange up to now. It is not clear who will exchange what information with whom unless no infrastructure is provided.

Article 2

Definitions

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

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

(a) it has potentially – apart from already designated National CSIRTs and/or SPoCs according to the provisions established through Directive (EU) 2022/2555 - also the capacity to act as a reference point and gateway to other public and private organisations at national level for collecting and analysing ~~information~~ on cyber threats and incidents and contributing to a Cross-border SOC collaboration platform;

Commented [RS71]: It should be made clear here that a SOC hub may not be the only organization at national level for collecting and analyzing information as well as acting as reference point/gateway for public and private organisations.

Overall it should be in MS decision whether it would define a SOC or a National CSIRT for this task, as outlined by NIS2. Please be aware of duplication and conflicting reporting lines w.r.t. NIS2 provisions.

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

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

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

(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;

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

(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;

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

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

(11) **(8a) 'trusted providers'** means managed security service providers as defined in Article 6, point (40), of Directive (EU) 2022/2555 selected in accordance with Article 16 of this Regulation.

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

Chapter II

THE EUROPEAN ~~CYBER SHIELD~~ CYBERSECURITY ~~ALERT~~ SUPPORTING SYSTEM

Article 3

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

1. An interconnected pan-European infrastructure **that consists** of **National SOC hubs and Cross-border SOC collaboration platforms joining on a voluntary basis** ~~Security Operations Centres ('European Cyber Shield~~ **the European Cybersecurity Alert System**~~')~~ shall be established to **support the** develop**ment of** advanced capabilities for the Union to

detect, analyse and process data on cyber threats and incidents in the Union. ~~It shall consist of all National Security Operations Centres ('National SOCs') and Cross-border Security Operations Centres ('Cross-border SOCs').~~

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

2. The European ~~Cyber Shield~~ **Cybersecurity** ~~**Alert**~~ **Supporting System** shall:

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

(b) **share** ~~**produce**~~ high-quality, actionable information and cyber threat intelligence, through the use of state-of-the art tools **and advanced technologies such as**~~, notably A~~**a**rtificial ~~**I**~~**i**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, namely the CSIRTs Network and** ~~**such as**~~ **competent authorities designated or established pursuant to Article 8 of Directive (EU) 2022/2555**~~**, CSIRTs and the CSIRTs network**~~;

~~(c)~~(d) regularly, and in any case, when significant incidents are concerned that fall under Art. 23 (1) of **Directive (EU) 2022/2555, share this information and data with the CSIRTs Network without undue delay;**

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

~~(e)~~(f) 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**~~ **Supporting 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**

Commented [AS72]: These tasks are partly achieved by CSIRTs NW. Please clarify allocation of tasks and complementarity of those between the new system and the existing CSIRTs NW.

Commented [RS73]: Formulate more specific

Formatted: Font: (Default) +Headings CS (Times New Roman), 12 pt

Formatted: Indent: Left: 0.69 cm, Hanging: 1 cm, Right: 0 cm, Space Before: 0 pt, Line spacing: single, No bullets or numbering, Tab stops: Not at 2.69 cm + 2.69

thereof.

Article 4

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 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~~ Supporting System** ~~National SOCs~~ shall be selected by the European Cybersecurity Competence Centre ('ECCC') to **take part** ~~participate~~ in a joint procurement of tools and infrastructures with the ECCC**, in order to set up National SOC hubs or enhance capabilities of an existing one**. The ECCC may award grants to the selected **Member States** ~~National SOCs~~ to fund the operation of those tools and infrastructures. The Union financial contribution shall cover up to 50% of the acquisition costs of the tools and infrastructures, and up to 50% of the operation costs, with the remaining costs to be covered by the Member State. Before launching the procedure for the acquisition of the tools and infrastructures, the ECCC and the **Member State** ~~National SOC~~ shall conclude a hosting and usage agreement regulating the usage of the tools and infrastructures.

3. A **Member State** ~~National SOC~~ selected pursuant to paragraph 2 shall commit to apply **for their National SOC hubs** to participate in a Cross-border SOC **collaboration Platform** within two years from the date on which the tools and infrastructures are acquired, or on which it receives grant funding, whichever occurs sooner. If a **Member State's** National SOC **hub** is not a participant in a Cross-border SOC **collaboration Platform** by that time, it can submit an application ~~**the Member State** **to participate** it shall not~~in order to be eligible for

additional Union support under this **Chapter** ~~Regulation~~.

Commented [RS74]: We ask for clarification: What means "additional Union support"? There should be a possibility for MS to apply for National SOC hubs after that date (2 years).

Article 5

Cross-border Security Operations Centre~~s~~ collaboration Platforms

1. A Hosting Consortium consisting of at least three Member States, ~~represented by National SOCs~~, committed to **ensuring that their National SOC hubs work** ~~working~~ together to

coordinate their cyber-detection and threat monitoring activities shall be eligible to participate in actions to establish a Cross-border SOC **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 and infrastructures with the ECCC. The ECCC may award to the Hosting Consortium a grant to fund the operation of the tools and infrastructures. The Union financial contribution shall cover up to 75% of the acquisition costs of the tools and infrastructures, and up to 50% of the operation costs, with the remaining costs to be covered by the Hosting Consortium. Before launching the procedure for the acquisition of the tools and infrastructures, the ECCC and the Hosting Consortium shall conclude a hosting and usage agreement regulating the usage of the tools and infrastructures.

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

4. A 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 Host**i**ng 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 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 and infrastructures already jointly procured with that Hosting Consortium.

Article 6

Cooperation and information sharing within and between cross-border SOCs ~~s~~ collaboration Platforms and the CSIRTs Network

Commented [RS75]: We think that the info sharing with the CSIRTs Network should be separately taken up here in order to highlight the importance of integrating the SOC platforms into existing structures for info sharing. See our proposal in Art. 3 (2 c + d)

1. Members of a Hosting Consortium shall **ensure that their National SOC hubs** exchange**, in accordance with the Consortium Agreement,** regularly exchange relevant information among themselves within the Cross-border SOC **collaboration Platform** and with the CSIRTs Network, and in any case, when significant incidents are concerned that fall under Art. 23 (1) of Directive (EU) 2022/2555, they shall share this information and data with the CSIRTs Network without undue delay; 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 prevent, detect, respond to or recover from incidents or to mitigate their impact;

   (b) enhances the level of cybersecurity, in particular through raising awareness in relation to cyber threats, limiting or impeding the ability of such threats to spread, supporting a range of defensive capabilities, vulnerability remediation and disclosure, threat detection, containment and prevention techniques, mitigation strategies, or response and recovery stages or promoting collaborative threat research between public and private entities.

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

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

   (b) a governance framework **clarifying and** incentivising the sharing of information **referred to in paragraph 1** by all participants;

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

3. To encourage exchange of information between Cross-border SOC~~s~~ **collaboration Platforms**, Cross-border SOC~~s~~ **collaboration Platforms** shall ensure a high level of interoperability between themselves. To facilitate the interoperability between the Cross-border SOC~~s~~ **collaboration Platforms**, the Commission may ~~prepare~~ issue ~~some~~ ~~guidance~~guidance documents on ~~the~~possible ~~, by means of implementing acts, after consulting the ECCC, specify the~~ conditions for this interoperability after consulting the

Formatted: Font: (Default) +Headings CS (Times New Roman), Bold

Commented [RS76]: Red line: no implementing acts

CSIRTs Network. ~~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 to the committee referred to in Article 21(1), the Commission shall consult the ECCC and existing Cross-border SOC collaboration Platforms.**~~

4. Cross-border SOC~~s~~ **collaboration 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. Where the Cross-border SOC~~s~~ **collaboration Platforms** obtain information relating to a potential or ongoing large-scale cybersecurity incident, they shall **ensure** ~~provide~~ **that** relevant information **is provided** to **the CSIRTs network,** 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 ~~without undue delay~~and with the respective Consortium Agreements.

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

Commented [RS77]: In our opinion there is no need for further implementing acts

Article 8

Security

1. Member States participating in the European ~~Cyber Shield~~ **Cybersecurity Alert System** shall ensure a high level of data security and physical security of the European ~~Cyber Shield~~ **Cybersecurity Alert System** infrastructure, and shall ensure that the infrastructure ~~shall be~~ **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**~~ **Supporting System** shall ensure that the sharing of 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.

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** paragraph**s** 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.

Chapter III

CYBER EMERGENCY MECHANISM

Article 9

Establishment of the Cyber Emergency Mechanism

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

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

Article 10

Type of actions

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

(a) preparedness actions**:**~~, including~~

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

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

(b) ~~response~~ actions~~,~~ supporting response to and **initiating** ~~immediate~~ recovery from significant and large-scale cybersecurity incidents, to be provided by trusted providers participating in the EU Cybersecurity Reserve established under Article 12;

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

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

Article 11

Coordinated preparedness testing of entities

1. For the purpose of supporting the coordinated preparedness testing of entities referred to in Article 10(1), point (a), across the Union, **and with due respect to the Member States competences,** the Commission, after consulting the NIS Cooperation Group and ENISA, shall identify the sectors, or sub-sectors, concerned, from the Sectors of High Criticality listed in Annex I to Directive (EU) 2022/2555 from which **Member States may voluntarily request to participate and to this end propose** entities to ~~may~~ be subject to the coordinated preparedness testing.~~,~~

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

2. The NIS Cooperation Group in cooperation with the Commission, ENISA, and the High Representative, shall develop common risk scenarios and methodologies for the **coordinated testing exercises under Article 10 (1) (a) (i). The NIS Cooperation Group, in cooperation with Commission, ENISA and the High Representative, may develop common risk**

scenarios and methodologies for other preparedness actions under Article 10(1)(a)(ii).

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, responding or providing support for responding to significant or large-scale cybersecurity incidents, and ~~immediate~~ **initiate** recovery from such incidents.

2. The EU Cybersecurity Reserve shall consist of incident response services from trusted providers selected in accordance with the criteria laid down in Article 16. The Reserve shall include pre-committed services. The ~~services~~ **Reserve shall** be deployable **upon request** in all Member States **and in third countries referred to in Article 17 (1).**

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

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

   (b) Union institutions, bodies and agencies.

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

4. Users referred to in paragraph 3, point (a), shall use the services **granted upon their request** from the EU Cybersecurity Reserve in order to respond or support response to and **initiate** ~~immediate~~ recovery from significant or large-scale incidents affecting entities operating in **sectors of high** critical**ity** or ~~**highly**~~ **other** critical sectors.

5. The Commission shall responsibility **have overall responsibility** for the implementation of the EU Cybersecurity Reserve. **To that end, the** Commission**, in cooperation with the NIS Cooperation Group and ENISA,** shall determine the priorities and evolution of the EU Cybersecurity Reserve, in line with the requirements of the users referred to in paragraph 3, and shall supervise its implementation, and ensure complementarity, consistency, synergies and links with other support actions under this Regulation as well as other Union actions and programmes. **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. For that purpose, ENISA shall be equipped with significant personnel resources.

7. ~~In order to support the Commission in establishing the EU Cybersecurity Reserve,~~ ENISA shall prepare a mapping of the services needed **and their availability**, after consulting **~~Member States~~ the NIS Cooperation Group** and the Commission. ENISA shall prepare a similar mapping, after consulting the **the NIS Cooperation Group and the** Commission, to identify the needs of third countries eligible for support from the EU Cybersecurity Reserve pursuant to Article 17. The Commission, where relevant, **may ~~shall~~ ~~seek the views of~~ ~~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). **Before submitting those drafting implementing acts to the committee referred to in Article 21(1), the Commission may exchange advice and cooperate with the NIS Cooperation Group.**

Article 13

Requests for support from the EU Cybersecurity Reserve

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

2. To receive support from the EU Cybersecurity Reserve, the users referred to in Article 12(3) shall take **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 from users referred to in Article 12(3), point (a), of this Regulation shall be transmitted **to the potential provider via a secure platform hosted by ENISA.** ~~to the Commission and ENISA via the Single Point of Contact designated or established by the Member State in accordance with Article 8(3) of Directive (EU) 2022/2555~~.

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

Commented [RS78]: The EU Cybersecurity Reserve has the potential to increase the level of resilience of EU MS and third countries. However, in its current form, it would make the process of responding to "significant or large scale incidents" very slow and bureaucratic.

Below, we propose a possible solution to streamline the process of requesting assistance from the EU Cybersecurity Reserve, with the goal of making this legislative proposal efficient and crisis-proof:

1. Through calls for tenders, the Commission will be able to establish a pool of qualified service providers ready to assist Member States and third countries in the event of a cyber-incident.
2. In order to streamline the request for assistance, the potential users should be able to directly connect with service providers through a secure platform which, through a filtering system (e.g. Location, Skills, Expertise, Language).
3. Through this platform, MS and third countries would be able to find quickly the right qualified expert in the field.
4. Providers, once contacted directly by the users, should accept or decline the request without undue delay.
5. Further details of the working agreement between the user and the provider should be regulated bilaterally.
6. The prioritization process, as proposed by the Commission, should take place only once the IPCR Mechanism is triggered:
   a. In the case of multiple concurrent requests, the following criteria shall be taken into account, where relevant (as specified under article 14).

this Article.

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

   (a) appropriate information regarding the affected entity and potential impacts of the incident **on affected Member State(s) and users, including the risk of spill over,** and the planned use of the requested support, including an indication of the estimated needs;

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

   (c) **where relevant, available** information about other forms of support available to the affected entity, including contractual arrangements in place for incident response and **initial** ~~immediate~~ recovery services, as well as insurance contracts potentially covering such type of incident.

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

6. ENISA, in cooperation with the Commission and the NIS Cooperation Group, shall develop a ~~template to facilitate the submission of~~ secure platform where direct requests for support from the EU Cybersecurity Reserve between applications and potential providers can take place.

7. The Commission may, by means of implementing acts, specify further the detailed arrangements for allocating the EU Cybersecurity Reserve support services. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2).

Article 14

Implementation of the support from the EU Cybersecurity Reserve

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

any event no later than 72 hours from the submission of the request to ensure effectiveness of the support action.

2. Providers process requests on a first-come, first-served basis. A response shall be transmitted to the users referred to in Article 12(3) without delay.

3. In situations, when the Integrated Political Crisis Response Mechanism ('IPCR') is triggered, and in the case of multiple concurrent requests, the Commission, in consultation with ENISA, ~~To~~ may support the deployment of the EU Cyber Reserve by ~~prioritis~~prioritizing~~e~~ such requests, in accordance with ~~in the case of multiple concurrent requests,~~ the following criteria ~~shall be taken into account, where relevant~~:

Formatted: List Paragraph,Listaszerű bekezdés1,List Paragraph à moi,Colorful List - Accent 11,Medium Grid 1 - Accent 21,Listaszeru bekezdés1,Colorful List - Accent 111,Dot pt,F5 List Paragraph,List Paragraph1,No Spacing1,List Paragraph Char Char Char,Bullets,L,3, Right: 1.02 cm, Line spacing: 1.5 lines, Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.69 cm + Indent at: 1.69 cm, No widow/orphan control, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Tab stops: 1.69 cm, Left + 1.69 cm, Left

(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 and Union institutions, bodies and agencies.

4. In case of such prioritization, the Commission should inform the Member States on the outcome of the decision, outlining which criteria were applied.

~~2.~~5. The EU Cybersecurity Reserve services shall be provided in accordance with specific agreements between the service provider and the user to which the support under the EU Cybersecurity Reserve is provided. Those agreements shall include liability conditions.

~~3.~~6. The agreements referred to in paragraph 3 may be based on templates prepared by ENISA, after consulting Member States.

~~4.~~7. The Commission and ENISA shall bear no contractual liability for damages caused to third parties by the services provided in the framework of the implementation of the EU Cybersecurity Reserve.

~~5.~~8. Within **three** ~~one~~ month**s** from the end of the support action, the users shall provide **the** Commission**,** ~~and~~ ENISA**, the CSIRTs network and, where appropriate, EU-CyCLONe** with a summary report about the service provided, results achieved and the lessons learned. When the user is from a third country as set out in Article 17, such report shall be shared with the High Representative.

~~6.~~9. The Commission shall report to the NIS Cooperation Group**, on a regular basis and at least once per year,** about the use and the results of the support~~, on a regular basis~~.

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.69 cm + Indent at: 1.69 cm

Formatted: Font: (Default) +Headings CS (Times New Roman), 12 pt, Not Bold

~~*Article 15*~~

~~Coordination with crisis management mechanisms~~

~~1. In cases where significant or large-scale cybersecurity incidents originate from or result in disasters as defined in Decision 1313/2013/EU[1], the support under this Regulation for responding to such incidents shall complementactions under and without prejudice to Decision 1313/2013/EU.~~

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

~~3. In consultation with the High Representative, support under the Cyber Emergency Mechanism may complement assistance provided in the context of the Common Foreign and Security Policy and Common Security and Defence Policy, including through the Cyber Rapid Response Teams. It may also complement or contribute to assistance provided by one Member State to another Member State in the context of Article 42(7) of the Treaty on the European Union.~~

~~4. Support under the Cyber Emergency Mechanism may form part of the joint response between the Union and Member States in situations referred to in Article 222 of the Treaty on the Functioning of the European Union.~~

Article 16

Trusted providers

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

   (a) ensure **that the services included in** the EU Cybersecurity Reserve **are such that the Reserve** ~~includes services that~~ may be deployed in all Member States, taking into account in particular national requirements for the provision of such services, including certification or accreditation;

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

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

(c) ensure that the EU Cybersecurity Reserve brings EU added value, by contributing to the objectives set out in Article 3 of Regulation (EU) 2021/694, including promoting the development of cybersecurity skills in the EU.

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

(a) the provider shall demonstrate that its personnel has the highest degree of professional integrity, independence, responsibility, and the requisite technical competence to perform the activities in their specific field, and ensures the permanence/continuity of expertise as well as the required technical resources;

(b) the provider, its subsidiaries and subcontractors shall have in place a framework to protect sensitive information relating to the service, and in particular evidence, findings and reports, and is compliant with Union security rules on the protection of EU classified information;

(c) the provider shall provide sufficient proof that its governing structure is transparent, not likely to compromise its impartiality and the quality of its services or to cause conflicts of interest;

(d) the provider shall have appropriate security clearance, at least for personnel intended for service deployment**~~:~~ 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.

Article 17

Support to DEP-associated third countries

1. **A DEP- associated t~~T~~**hird countr**y~~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 shall be 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 associated third countries eligible to receive services from the EU Cybersecurity Reserve shall include competent authorities such as CSIRTs and cyber crisis management authorities.

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

5. **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, p~~P~~**rior to receiving any support from the EU Cybersecurity Reserve, third countries shall provide to the Commission **~~and the High Representative~~** information about their cyber resilience and risk management capabilities, including at least information on national measures taken to prepare for significant or large-scale cybersecurity incidents, as well as information on responsible national entities, including CSIRTs or equivalent entities, their capabilities and the resources allocated to them. **The Commission shall share this information with the High Representative, for the purpose**

of facilitating the cooperation referred to in paragraph 6. Where provisions of Articles 13

and 14 of this Regulation refer to Member States, they shall apply to third countries as set out in paragraph 1.

6. The Commission shall **inform the NIS Cooperation Group ~~Council~~ and cooperate** ~~coordinate~~ with the High Representative about the requests received and the implementation of the support granted to third countries from the EU Cybersecurity Reserve. **The Commission shall take into account the opinions of the NIS Cooperation Group and the High Representative, if such are provided.**

Article 17a) ~~15~~

Coordination with Union crisis management mechanisms

1. **~~In cases w~~Where a significant cybersecurity incident or a large-scale cybersecurity incident~~s~~ originate~~s~~ from or result~~s~~ in a disaster~~s~~ as defined in Article 4, point (1), of Decision No 1313/2013/EU[1], 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~~, 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.**

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.**~~

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

Chapter IV

CYBERSECURITY INCIDENT REVIEW MECHANISM

Article 18

Cybersecurity Incident Review Mechanism

1. ~~**After consulting Member States concerned, and A**~~at the request of the Commission, the EU-CyCLONe or the CSIRTs network, **and with the agreement of the Member States concerned,** ENISA shall review and assess threats, vulnerabilities and mitigation actions with respect to a specific significant or large-scale cybersecurity incident. Following the completion of a review and assessment of an incident, ENISA shall deliver an incident review report to the CSIRTs network, the EU-CyCLONe and the Commission to support them in carrying out their tasks, in particular in view of those set out in Articles 15 and 16 of Directive (EU) 2022/2555. ~~**Where relevant, **~~**When an incident has an impact on a third country**, the Commission shall share the report with the High Representative.

2. To prepare the incident review report referred to in paragraph 1, ENISA shall collaborate all relevant stakeholders, including representatives of Member States, the Commission, other relevant EU institutions, bodies and agencies, managed security services providers and users of cybersecurity services. Where appropriate, **and** ~~**in close cooperation**~~ **with the agreement 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, 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) 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 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 and Cross-border SOCs ~~s~~ **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';

(b) Paragraph 2 is replaced by the following:

'2. The actions under Specific Objective 3 shall be implemented primarily through the European Cybersecurity Industrial, technology and research Competence Centre and the Network of National Coordination Centres, in accordance with Regulation (EU) 2021/887 of the European Parliament and of the Council[1] with the exception of actions implementing the EU Cybersecurity Reserve, which shall be implemented by the Commission and ENISA.**';**

(2) Article 9 is amended as follows:

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

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

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

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

(b) the following paragraph 8 is added:

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

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

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

---

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

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.

[...]

ESTONIA

[…]

Whereas:

[…]

(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[27], it is necessary to increase the resilience of citizens, businesses and entities operating critical infrastructures against the growing cybersecurity threats, which can have devastating societal and economic impacts. Therefore, investment in infrastructures and services that will support faster detection and response to cybersecurity threats and incidents is needed, and Member States need assistance in better preparing for, as well as responding to significant and large-scale cybersecurity incidents. **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.

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

[…]

(7) It is necessary to strengthen the detection and situational awareness of cyber threats and incidents throughout the Union and to strengthen solidarity by enhancing Member States' and the Union's preparedness and capabilities to respond to significant and large-scale cybersecurity incidents. Therefore a pan-European infrastructure of SOCs (European Cyber**security** ~~Shield~~ **Alert System**) should be deployed 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**, with due respect for Member State competences and without duplication of the activities conducted by the CSIRT network, EU-CyCLONe and the NIS Cooperation Group**. These actions shall be without prejudice to Articles 107 and 108 of the Treaty on the Functioning of the European Union ('TFEU').

(8) To achieve these objectives, it is also necessary to amend Regulation (EU) 2021/694 of the European Parliament and of the Council[28] 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 DEP, which aims at guaranteeing the resilience, integrity and trustworthiness of the Digital Single Market, at strengthening capacities to monitor cyber-attacks and threats and to respond to them, and at reinforcing cross-border cooperation on cybersecurity. This will be complemented by the specific conditions under which financial support may be granted for those actions should be established and the governance and coordination mechanisms necessary in order to achieve the intended objectives should be defined. Other amendments to Regulation (EU) 2021/694 should include descriptions of proposed actions under the new operational objectives, as well as measurable indicators to monitor the implementation of these new operational objectives.

[…]

(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

---

28 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).

infrastructures on the territory of the Union, including their geographical distribution, interconnection and potential effects in case of cyber-attacks affecting those infrastructures. A large-scale Union infrastructure of SOCs should be deployed ('the European Cyber**security** ~~Shield~~ **Alert System**'), comprising of several interoperating cross-border platforms, each grouping together several National CSIRT ~~SOCs~~ hubs. That infrastructure should serve national and Union cybersecurity interests and needs, leveraging state of the art technology for advanced data collection and analytics tools, enhancing cyber detection and management capabilities and providing real-time situational awareness. That infrastructure should serve to increase detection of cybersecurity threats and incidents and thus complement and support Union entities and networks responsible for crisis management in the Union, notably the EU Cyber Crises Liaison Organisation Network ('EU-CyCLONe'), as defined in Directive (EU) 2022/2555 of the European Parliament and of the Council[29].

(13) **Participation in the European ~~Cyber Shield~~ Cybersecurity Alert System should be voluntary for Member States.** Each Member State **that decides to join the European ~~Cyber Shield~~ Cybersecurity Alert System** should designate a **National ~~SOC~~ ~~SOC~~ CSIRT hub.** ~~public body at national level tasked with coordinating cyber threat detection activities in that Member State.~~ These National SOC~~s~~ **hubs** should **have** ~~act~~ as **functionalities the capacity to act as** a reference point and gateway at national level for participation in the European ~~Cyber Shield~~ **Cybersecurity Alert System** and should **be capable of detecting, aggregating and analysing data relevant to cyber threats and incidents, by using in particular state-of-the-art technologies and that would be shared appropriately with the CSIRT network in order to support the network 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 or existing national platforms 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.**

Commented [A79]: This task should be fulfilled by national CSIRTs.Same for the rest of the text.

Formatted: Font: (Default) +Headings CS (Times New Roman), Underline

Formatted: Font: (Default) +Headings CS (Times New Roman), Strikethrough

Formatted: Font: (Default) +Headings CS (Times New Roman), Underline

[29] 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).

(14) As part of the European Cyber**security Alert System** ~~Shield~~, a number of Cross-border Cybersecurity Operations Centres ('Cross-border SOCs') should be established. These should bring together National ~~SOCs~~ CSIRTs from at least three Member States, so that the benefits of cross-border threat detection and information sharing and management can be fully achieved. The general objective of Cross-border SOCs should be to strengthen capacities to analyse, prevent and detect cybersecurity threats and to support the production of high-quality intelligence on cybersecurity threats, notably through the sharing of **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.

(14a) A Member State selected by the European Cybersecurity Competence Centre (ECCC) following a call for expression of interest to set up a National SOC Hub or enhance the capabilities of an existing one, should jointly purchase relevant tools and infrastructures with the ECCC. Such a Member State should be eligible to receive a grant to operate the tools and infrastructures. 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 collaboration SOC Platform or enhance the capabilities of an existing one, should jointly purchase relevant tools and infrastructures with the ECCC. Such a Hosting Consortium should be eligible to receive a grant to operate the tools and infrastructures. 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 procurement procedure to purchase the relevant tools and infrastructures should be carried out jointly by the ECCC and relevant contracting authorities from the Member States selected following these calls for expressions of interest. Private entities should therefore not be eligible to participate in the calls for expression of interest to jointly purchase tools and infrastructures with the ECCC, or to receive grants to operate those tools and infrastructures. However, the Member States should have the possibility to involve private entities in the setting up, enhancement and operation of their National SOC Hubs and Cross-border ~~SOCs~~ Platforms in other ways which they deem appropriate, in compliance with national and Union law.

Formatted: Font: (Default) +Headings CS (Times New Roman), Strikethrough

Formatted: Font: (Default) +Headings CS (Times New Roman), Underline

Formatted: Font: (Default) +Headings CS (Times New Roman), Strikethrough

(15) At national level, the monitoring, detection and analysis of cyber threats is typically ensured by SOCs of public and private entities, in combination with CSIRTs. In addition, CSIRTs exchange information in the context of the CSIRT network, in accordance with Directive (EU) 2022/2555. The Cross-border SOCs should constitute a new capability that is complementary to the CSIRTs network **and will cooperate closely with it,** by pooling **data** and sharing **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.

[…]

(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 SOC Platforms obtain information related to a potential or ongoing large-scale cybersecurity incident, theuy should provide relevant information to the CSIRTs network. ~~Recommendation (EU) 2017/1584 on coordinated response to large-scale cybersecurity incidents and crises addresses the role of all relevant actors. Directive (EU) 2022/2555 also recalls the Commission's responsibilities in the Union Civil Protection Mechanism ('UCPM') established by Decision 1313/2013/EU of the European Parliament and of the Council, as well as for providing analytical reports for the Integrated Political Crisis Response Mechanism ('IPCR') arrangements under Implementing Decision (EU) 2018/1993. Therefore, in situations where Cross-border SOCs obtain information related to a potential or ongoing large-scale cybersecurity incident, they should provide relevant information to EU-CyCLONe, the CSIRTs network and the Commission. In particular, depending on the situation, information to be shared could include technical information, information about the nature and motives of the attacker or potential attacker, and higher-level non-technical information about a potential or ongoing large-scale cybersecurity incident.~~ In this context, due regard should be paid to the need-to-know principle and to the potentially sensitive nature of the information shared. In accordance with Directive (EU)

Formatted: Font: (Default) +Headings CS (Times New Roman), Underline

Formatted: Font: (Default) +Headings CS (Times New Roman), Strikethrough

Formatted: Font: (Default) +Headings CS (Times New Roman), Underline

2022/2555 the CSIRTs network will, if relevant, inform EU-CyCLONe on the basis of their agreed procedural arrangements for cooperation. As EU-CyCLONe consists of the representatives of Member States' cyber crisis management authorities as well as, in cases where a potential or ongoing large-scale cybersecurity incident has or is likely to have a significant impact on services and activities falling within the scope of this Directive, the Commission, the information from a Cross-border SOC Platform will be distributed through the existing cybercrisismanagement structures in the Union.

(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**~~ cause**s** ~~**and impacts** of cybersecurity~~ **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 should be able to issue guidance in this respect.** This should make it possible to improve collective detection capacities and timely warnings to authorities and relevant entities, notably by using the latest artificial intelligence and data analytics technologies.

(20) By collecting, **correlating,** sharing and exchanging **data and information**, the European ~~Cyber Shield~~ **Cybersecurity Alert System** should enhance the Union's technological sovereignty. The pooling of high-quality curated data should also contribute to the development of advanced artificial intelligence and data analytics technologies. It should be facilitated through the connection of the European ~~Cyber Shield~~ **Cybersecurity Alert System** with the pan-European High Performance Computing infrastructure established by Council Regulation (EU) 2021/1173[30].

[30] 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).

(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 'High Representative'), should gradually develop dedicated protocols and standards to allow for cooperation with the cyber defence community, including vetting and security conditions. The development of the European Cyber**security 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.

(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.

~~**(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 cybersecurity incidents and complement Member States' actions through emergency financial support for preparedness, response and **initial ~~immediate~~** recovery of essential services. That instrument should enable the rapid deployment of assistance in defined circumstances and under clear conditions and allow for a careful monitoring and evaluation of how resources have been used. Whilst the primary responsibility for preventing, preparing for and responding to cybersecurity incidents and crises lies with the Member States, the Cyber Emergency Mechanism promotes solidarity between Member States in accordance with Article 3(3) of the Treaty on European Union ('TEU').

(25) The Cyber Emergency Mechanism should provide support to Member States complementing their own measures and resources, and other existing support options in case of response to and **~~immediate~~ 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[31] **~~and Hybrid Rapid Response Teams~~**. It should address the need to ensure that specialised means are available to support preparedness and response to cybersecurity incidents across the Union and in third countries.

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

(26) This ~~instrument~~**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~~[32], **the EU Integrated Political Crisis Response Arrangements under Council Implementing Decision (EU) 2018/1993**~~IPCR~~[33] **(IPCR Arrangements), Commission Recommendation 2017/1584**[34] 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. 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.

[…]

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

---

32 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).

33 **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.~~

34 **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).**

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 functioning of essential services.

(29) As part of the preparedness actions, to promote a consistent approach and strengthen security across the Union and its internal market, support should be provided for testing and assessing cybersecurity of entities operating in ~~**highly critical**~~ sectors **of high criticality** identified pursuant to Directive (EU) 2022/2555 in a coordinated manner. For this purpose, the Commission, with the support of ENISA and in cooperation with the NIS Cooperation Group established by Directive (EU) 2022/2555, should regularly identify relevant sectors or subsectors, which should be eligible to receive financial support for coordinated testing at Union level. The sectors or subsectors should be selected from Annex I to Directive (EU) 2022/2555 ('Sectors of High Criticality'). The coordinated testing exercises should be based on common risk scenarios and methodologies. The selection of sectors and development of risk scenarios should take into account relevant Union-wide risk assessments and risk scenarios, including the need to avoid duplication, such as the risk evaluation and risk scenarios called for in the Council conclusions on the development of the European Union's cyber posture ~~to be~~ conducted by the Commission, the High Representative and the NIS Cooperation Group, in coordination with relevant civilian and military bodies and agencies and established networks, including the EU CyCLONe, as well as the risk assessment of communications networks and infrastructures requested by the Joint Ministerial Call of Nevers and conducted by the NIS Cooperation Group, with the support of the Commission and ENISA, and in cooperation with the Body of European Regulators for Electronic Communications (BEREC), the coordinated risk assessments to be conducted under Article 22 of Directive (EU) 2022/2555 and digital operational resilience testing as provided for in Regulation (EU) 2022/2554 of the European Parliament and of the Council[35]. 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

[35] 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

entities operating in ~~**highly critical**~~ sectors **of high criticality**. 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.

[…]

(33) 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 or large-scale cybersecurity incidents. The EU Cybersecurity Reserve should ensure the availability and readiness of services. The services from the EU Cybersecurity Reserve should serve to support national authorities in providing assistance to affected entities operating in **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, Member States should specify the support provided to the affected entity at the national level, which should be taken into account when assessing the Member State request. **The CSIRT Network established in Directive EU 2022/2555 can advise the Commission in 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.

(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, ENISA may be the contracting authority for those services with whose operation and administration it has been entrusted. The procurement procedures to establish the EU Cybersecurity Reserve should be conducted in accordance with Regulation EU 2018/1046. 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 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. 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 in 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 Cyber 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 NIS Cooperation Group, the Commission should ensure that the views of Member States as regards priorities and 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.

(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,** 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 relevant stakeholders, including representatives from the private sector, Member States, the Commission and other relevant EU institutions, bodies and agencies. As regards the private sector, ENISA is developing channels for exchanging information with specialised providers, including providers of managed security solutions and vendors, in order to contribute to ENISA's mission of achieving a high common level of cybersecurity across the Union. Building on the collaboration with stakeholders, including the private sector, the review report on specific incidents should aim at assessing the causes, impacts and mitigations of an incident, after it has occurred. Particular attention should be paid to the input and lessons shared by the managed security service providers that fulfil the conditions of highest professional integrity, impartiality and requisite technical expertise as required by this Regulation. The report should be delivered and feed into the work of the EU~~=~~-CyCLONe, the CSIRTs network and the Commission. When the incident relates to a third country, it **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 as a whole. Therefore, third countries associated to the DEP may be supported from the EU Cybersecurity Reserve, where this is provided for in the ~~respective association~~ **relevant** agreement **or Association Council decision through which ~~to~~ the third country is associated** to DEP. **The CSIRT Network established in Directive EU 2022/2555 can advise the Commission in reviewing requests for support from the EU Cybersecurity Reserve.** 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~~.

(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.

[…]

HAVE ADOPTED THIS REGULATION:

Chapter I

GENERAL OBJECTIVES, SUBJECT MATTER, AND DEFINITIONS

Article 1

Subject-matter and objectives

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

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

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

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

2. This Regulation pursues the objective to strengthen solidarity at Union level **and enhance Member States cyber resilience** through **the** following specific objectives:

   […]

   (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 capacities **to handle** ~~against~~ significant or large-scale cybersecurity incidents, including by making Union cybersecurity incident response

support available for third countries associated to the Digital Europe Programme ('DEP');

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

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

4. Without prejudice to Article 346 TFEU, the 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 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.

Article 2

Definitions

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

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

~~(a) it has the capacity to act as a reference point and gateway to other public and private organisations at national level for collecting and analysing information on cyber threats and incidents and contributing to a Cross-border SOC 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 Security Operations Centre collaboration Platform' ("Cross-border SOC collaboration Platform**") means a multi-country platform, **established by a written consortium agreeement** that brings together in a coordinated network structure **N~~n~~**ational

Formatted: Font: (Default) +Headings CS (Times New Roman), Strikethrough

Formatted: Font: (Default) +Headings CS (Times New Roman), Strikethrough

CSIRTs ~~SOCs~~ ~~**Hubs**~~ from at least three Member States ~~who form a Hosting Consortium~~, and that is designed to **monitor, detect and analyse** ~~prevent~~ cyber threats ~~and~~ **to prevent** incidents and to support the production of **cyber threat** ~~high-quality~~ intelligence, notably through the exchange of **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[36];~~

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

(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;

(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;

~~(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;~~

Formatted: Font: (Default) +Headings CS (Times New Roman), Underline

Formatted: Font: (Default) +Headings CS (Times New Roman), Strikethrough

Formatted: Font: (Default) +Headings CS (Times New Roman), Strikethrough

Formatted: Font: (Default) +Headings CS (Times New Roman), Strikethrough

Formatted: Font: (Default) +Headings CS (Times New Roman), Underline

[36] 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).

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

~~(11)~~ **(8a) 'trusted providers'** means managed security service providers as defined in Article 6, point (40), of Directive (EU) 2022/2555 selected in accordance with Article 16 of this Regulation.

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

Chapter II

THE EUROPEAN ~~CYBER SHIELD~~ CYBERSECURITY ALERT SYSTEM

Article 3

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

1. An interconnected pan-European infrastructure **that consists** of ~~**National SOC hubs and Cross-border SOC**~~ **collaboration platforms joining on a voluntary basis** ~~Security Operations Centres ('European Cyber Shield~~ **the European Cybersecurity Alert System**~~')~~ shall be established to **support the** develop**ment of** advanced capabilities for the Union to detect, analyse and process data on cyber threats and incidents in the Union. ~~It shall consist of all National Security Operations Centres ('National SOCs') and Cross-border Security Operations Centres ('Cross-border SOCs').~~

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

2. The European ~~Cyber Shield~~ **Cybersecurity Alert System** shall:

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

   (b) **share** ~~**produce**~~ high-quality, actionable information and cyber threat intelligence, through the use of state-of-the art tools **and advanced technologies such as**~~, notably A~~**a**rtificial ~~**I**~~**i**ntelligence and data analytics**, and share that information and cyber threat intelligence** ~~technologies~~;

Formatted: Font: (Default) +Headings CS (Times New Roman), Strikethrough

Formatted: Font: (Default) +Headings CS (Times New Roman), Strikethrough

Formatted: Font: (Default) +Headings CS (Times New Roman), Strikethrough

(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, CSIRTs and the CSIRTs network;

(d) contribute to enhanced ~~faster~~ detection of cyber threats and 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 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 designate at least one National CSIRT ~~SOC~~ **Hub**. ~~The National SOC shall be a public body.~~

~~It shall have the capacity to act as a reference point and gateway to other public and private organisations at national level for collecting and analysing information on cybersecurity threats and incidents and contributing to a Cross-border SOC. It shall be equipped with state-of-the-art technologies capable of detecting, aggregating, and analysing data relevant to cybersecurity threats and incidents.~~

2. Following a call for expression of interest, **Member States intending to participate in the European ~~Cyber Shield~~ Cybersecurity Alert System** ~~National SOCs~~ shall be selected by the European Cybersecurity Competence Centre ('ECCC') to **take part** ~~participate~~ in a joint procurement of tools and infrastructures with the ECCC**, in order to set up National CSIRT ~~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

Formatted: Font: (Default) +Headings CS (Times New Roman), Underline

Formatted: Font: (Default) +Headings CS (Times New Roman), Strikethrough

Formatted: Font: (Default) +Headings CS (Times New Roman), Underline

Formatted: Font: (Default) +Headings CS (Times New Roman), Strikethrough

costs of the tools and infrastructures, and up to 50% of the operation costs, with the remaining costs to be covered by the Member State. Before launching the procedure for the acquisition of the tools and infrastructures, the ECCC and the **Member State** ~~National SOC~~ shall conclude a hosting and usage agreement regulating the usage of the tools and infrastructures.

3. A **Member State** ~~National SOC~~ selected pursuant to paragraph 2 shall commit to apply **for their National** CSIRT **~~SOC~~ hubs** to participate in a Cross-border ~~SOC~~ **collaboration Platform** within two years from the date on which the tools and infrastructures are acquired, or on which it receives grant funding, whichever occurs sooner. If a **Member State's** National SOC **hub** is not a participant in a Cross-border SOC **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 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** CSIRT **~~SOC~~ hubs work** ~~working~~ together to coordinate their cyber-detection and threat monitoring activities shall be eligible to participate in actions to establish a Cross-border ~~SOC~~ **collaboration Platform**.

[…]

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.

4. A 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 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

Formatted: Font: (Default) +Headings CS (Times New Roman), Strikethrough

Formatted: Font: (Default) +Headings CS (Times New Roman), Strikethrough

Formatted: Font: (Default) +Headings CS (Times New Roman), Strikethrough

Formatted: Font: (Default) +Headings CS (Times New Roman), Strikethrough

Formatted: Font: (Default) +Headings CS (Times New Roman), Strikethrough

shall not affect the ECCC's ownership rights over the tools and infrastructures already jointly procured with that Hosting Consortium.

Article 6

Cooperation and information sharing within and between cross-border ~~SOCs~~ collaboration Platforms

1. Members of a Hosting Consortium shall **ensure that their National ~~SOC~~ CSIRT hubs** exchange**, in accordance with the Consortium Agreement,** relevant information among themselves within the 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:

   […]

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

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

   (b) a governance framework **clarifying and** incentivising the sharing of information **referred to in paragraph 1** by all participants;

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

3. To encourage exchange of information between Cross-border ~~SOCs~~ **collaboration Platforms**, Cross-border ~~SOCs~~ **collaboration Platforms** shall ensure a high level of interoperability between themselves. To facilitate the interoperability between the Cross-border SOC~~s~~ **collaboration Platforms**, the Commission may, by means of implementing acts~~**, after consulting the ECCC,**~~ specify the conditions for this interoperability. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2) of this Regulation. **Before submitting those draft guidelines ~~implementing~~ acts to the committee referred to in Article 21(1), the Commission shall consult the CSIRTs Network ~~ECCC~~ and existing Cross-border SOC collaboration Platforms.**

Formatted: Font: (Default) +Headings CS (Times New Roman), Strikethrough

Formatted: Font: (Default) +Headings CS (Times New Roman), Strikethrough

Formatted: Font: (Default) +Headings CS (Times New Roman), Underline

Formatted: Font: (Default) +Headings CS (Times New Roman), Strikethrough

Formatted: Font: (Default) +Headings CS (Times New Roman), Strikethrough

Formatted: Font: (Default) +Headings CS (Times New Roman), Strikethrough

Formatted: Font: (Default) +Headings CS (Times New Roman), Strikethrough

Formatted: Font: (Default) +Headings CS (Times New Roman), Strikethrough

4. Cross-border SOC~~s~~ **collaboration 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. Where the Cross-border ~~SOCs~~ ~~SOCs~~ **collaboration Platforms** obtain information relating to a potential or ongoing large-scale cybersecurity incident, they shall **ensure** ~~provide~~ **that** relevant information **is provided** to **the CSIRTs network,** ~~EU-CyCLONe, the CSIRTs network, and the Commission, in view of their respective crisis management roles in accordance with Directive (EU) 2022/2555 without undue delay.~~

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

2. Each Cross-border collaboration Platform shall ensure that they have procedural arrangements for the information sharing in paragraph 1.

Article 8

Security

1. Member States participating in the European ~~Cyber Shield~~ **Cybersecurity Alert System** shall ensure a high level of data security and physical security of the European ~~Cyber Shield~~ **Cybersecurity Alert System** infrastructure, and shall ensure that the infrastructure ~~shall be~~ **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 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.

3. ~~The Commission may **adopt implementing acts** **issue guidance documents** **laying down technical requirements for Member States to comply with their obligation under~~

Formatted: Font: (Default) +Headings CS (Times New Roman), Strikethrough

Formatted: Font: (Default) +Headings CS (Times New Roman), Strikethrough

Formatted: Font: (Default) +Headings CS (Times New Roman), Strikethrough

Formatted: Font: (Default) +Headings CS (Times New Roman), Strikethrough

Formatted: Font: (Default) +Headings CS (Times New Roman), Strikethrough

Formatted: Font: (Default) +Headings CS (Times New Roman), Not Strikethrough

Formatted: Font: (Default) +Headings CS (Times New Roman), Underline

Formatted: Font: (Default) +Headings CS (Times New Roman), Underline

Formatted: Font: (Default) +Headings CS (Times New Roman), Strikethrough

Formatted: Font: (Default) +Headings CS (Times New Roman), Strikethrough

Formatted: Font: (Default) +Headings CS (Times New Roman), Strikethrough

Formatted: Font: (Default) +Headings CS (Times New Roman), Strikethrough

~~clarifying the application of~~ paragraph~~s~~ 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.

Formatted: Font: (Default) +Headings CS (Times New Roman), Strikethrough

Formatted: Font: (Default) +Headings CS (Times New Roman), Strikethrough

Chapter III

CYBER EMERGENCY MECHANISM

Article 9

Establishment of the Cyber Emergency Mechanism

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

[…]

Article 10

Type of actions

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

(a) preparedness actions**:**~~, including~~

(v) the coordinated preparedness testing of entities operating in **sectors of high criticality** ~~highly critical sectors~~ across the Union;

(vi) other preparedness actions for entities operating in sectors of high criticality ~~critical~~ and other ~~highly~~ critical sectors, including those involving exercises and trainings and ;

(b) ~~response~~ actions~~,~~ supporting response to and **initiating** ~~immediate~~ recovery from significant and large-scale cybersecurity incidents, to be provided by trusted providers participating in the EU Cybersecurity Reserve established under Article 12;

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

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

Article 11

Coordinated preparedness testing of entities

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

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

2. The NIS Cooperation Group in cooperation with the Commission, ENISA, and the High Representative, shall develop common risk scenarios and methodologies for the **coordinated testing exercises under Article 10 (1) (a) (i). The NIS Cooperation Group, in cooperation with Commission, ENISA and the High Representative, may develop common risk scenarios and methodologies for other preparedness actions under Article 10(1)(a)(ii).**

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, responding or providing support for responding to significant or large-scale cybersecurity incidents, and ~~immediate~~ **initiate** recovery from such incidents.

2. The EU Cybersecurity Reserve shall consist of incident response services from trusted providers selected in accordance with the criteria laid down in Article 16. The Reserve shall

include pre-committed services. The ~~services~~ **Reserve shall** be deployable **upon request** in all Member States **and in third countries referred to in Article 17 (1).**

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

   […]

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

4. Users referred to in paragraph 3, point (a), shall use the services **granted upon their request** from the EU Cybersecurity Reserve in order to respond or support response to and **initiate** ~~immediate~~ recovery from significant or large-scale incidents affecting entities operating in **sectors of high** critical**ity** or ~~**highly**~~ **other** critical sectors.

5. The Commission shall responsibility **have overall responsibility** for the implementation of the EU Cybersecurity Reserve. **To that end, the** Commission**, in cooperation with the NIS Cooperation Group and ENISA,** shall determine the priorities and evolution of the EU Cybersecurity Reserve, in line with the requirements of the users referred to in paragraph 3, and shall supervise its implementation, and ensure complementarity, consistency, synergies and links with other support actions under this Regulation as well as other Union actions and programmes. **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 a mapping of the services needed **and their availability**, after consulting ~~**Member States**~~ **the NIS Cooperation Group** and the Commission. ENISA shall prepare a similar mapping, after consulting the **the NIS Cooperation Group and the** Commission, to identify the needs of third countries eligible for support from the EU Cybersecurity Reserve pursuant to Article 17. The Commission, where relevant, **may** ~~shall~~ **seek the views of** ~~**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). **Before submitting those drafting implementing acts to the committee referred to in Article 21(1), the Commission may exchange advice and cooperate with the NIS Cooperation Group.**

Article 13

Requests for support from the EU Cybersecurity Reserve

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

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

[…]

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

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

   (a) appropriate information regarding the affected entity and potential impacts of the incident **on affected Member State(s) and users, including the risk of spill over,** and the planned use of the requested support, including an indication of the estimated needs;

   […]

   (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.

[…]

Article 14

Implementation of the support from the EU Cybersecurity Reserve

1. Requests for support from the EU Cybersecurity Reserve, shall be assessed by the Commission, with the support of ENISA or as defined in contribution agreements under Article 12(6), and a response shall be transmitted to the users referred to in Article 12(3) without delay **and in any event no later than 72 hours from the submission of the request to ensure effectiveness of the support action**.

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

   […]

   (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 and Union institutions, bodies and agencies.

[…]

6. Within **three** ~~one~~ month**s** from the end of the support action, the users shall provide **the** Commission**,** ~~and~~ ENISA**, the CSIRTs network and, where appropiate, EU-CyCLONe** with a summary report about the service provided, results achieved and the lessons learned. When the user is from a third country as set out in Article 17, such report shall be shared with the High Representative.

7. The Commission shall report to the NIS Cooperation Group**, on a regular basis and at least once per year,** about the use and the results of the support~~, on a regular basis~~.

~~*Article 15*~~

~~**Coordination with crisis management mechanisms**~~

~~1. In cases where significant or large-scale cybersecurity incidents originate from or result in disasters as defined in Decision 1313/2013/EU[37], 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~~

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

~~responding to such incident shall be handled in accordance with relevant protocols and procedures under the IPCR.~~

~~3. In consultation with the High Representative, support under the Cyber Emergency Mechanism may complement assistance provided in the context of the Common Foreign and Security Policy and Common Security and Defence Policy, including through the Cyber Rapid Response Teams. It may also complement or contribute to assistance provided by one Member State to another Member State in the context of Article 42(7) of the Treaty on the European Union.~~

~~4. Support under the Cyber Emergency Mechanism may form part of the joint response between the Union and Member States in situations referred to in Article 222 of the Treaty on the Functioning of the European Union.~~

Article 16

Trusted providers

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

   (a) ensure **that the services included in** the EU Cybersecurity Reserve **are such that the Reserve** ~~includes services that~~ may be deployed in all Member States, taking into account in particular national requirements for the provision of such services, including certification or accreditation;

   […]

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

   […]

   (d) the provider shall have appropriate security clearance, at least for personnel intended for service deployment~~;~~**, where required by a Member State;**

   […]

   (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.

Formatted: Font: (Default) +Headings CS (Times New Roman), Strikethrough

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 shall be 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.

[…]

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**, p~~P~~rior to receiving any support from the EU Cybersecurity Reserve, third countries shall provide to the Commission **~~and the High Representative~~** information about their cyber resilience and risk management capabilities, including at least information on national measures taken to prepare for significant or large-scale cybersecurity incidents, as well as information on responsible national entities, including CSIRTs or equivalent entities, their capabilities and the resources allocated to them. **The Commission shall share this information with the High Representative, for the purpose of facilitating the cooperation referred to in paragraph 6**. Where provisions of Articles 13 and 14 of this Regulation refer to Member States, they shall apply to third countries as set out in paragraph 1.

6. The Commission shall **inform the NIS Cooperation Group ~~Council~~ and cooperate~~coordinate~~** with the High Representative about the requests received and the implementation of the support granted to third countries from the EU Cybersecurity Reserve.

The Commission shall take into account the opinions of the NIS Cooperation Group and the High Representative, if such are provided.

Article 17a) ~~15~~

Coordination with Union crisis management mechanisms

1. **~~In cases w~~Where a significant cybersecurity incident or a large-scale cybersecurity incident~~s~~ originate~~s~~ from or result~~s~~ in a disaster~~s~~ as defined in Article 4, point (1), of Decision No 1313/2013/EU[38], 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~~, 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.**

~~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

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

1. ~~**After consulting Member States concerned, and A**~~at the request of the Commission, the EU-CyCLONe or the CSIRTs network, **and with the agreement of the Member States concerned,** ENISA shall review and assess threats, vulnerabilities and mitigation actions with respect to a specific significant or large-scale cybersecurity incident. Following the completion of a review and assessment of an incident, ENISA shall deliver an incident review report to the CSIRTs network, the EU-CyCLONe and the Commission to support them in carrying out their tasks, in particular in view of those set out in Articles 15 and 16 of Directive (EU) 2022/2555. ~~**Where relevant,**~~ **When an incident has an impact on a third country**, the Commission shall share the report with the High Representative.

2. To prepare the incident review report referred to in paragraph 1, ENISA shall collaborate all relevant stakeholders, including representatives of Member States, the Commission, other relevant EU institutions, bodies and agencies, managed security services providers and users of cybersecurity services. Where appropriate, **and ~~in close cooperation~~ with the agreement 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, 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) 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 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 and Cross-border **CSIRTs** ~~SOCs~~ **collaboration** platforms that contribute to situational awareness in the Union and to enhancing the cyber threat intelligence capacities of the Union';

[…]

(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.

[…]

Formatted: Font: (Default) +Headings CS (Times New Roman), Bold, Underline

Formatted: Font: (Default) +Headings CS (Times New Roman), Strikethrough

IRELAND

Chapter III

CYBER EMERGENCY MECHANISM

Article 9

Establishment of the Cyber Emergency Mechanism

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

2. Actions implementing the Cyber Emergency Mechanism shall be supported by funding from DEP and implemented in accordance with Regulation (EU) 2021/694 and in particular Specific Objective 3 thereof.- Article 12(5) of Regulation (EU) 2021/694 shall not be invoked if the limitation is likely to result in an absence of providers trusted by users of the services of a Member State, as set out in Article 12(3).

Commented [A80]: It needs to be explicit that Article 12(5) will not be applied in all circumstances. The decision to leave it to DEP Work Programme is not sufficient to see the Reserve being used in all Member States. An impact assessment that involved looking at the various situations in the Member States would have identified this as an issue.

Article 16

Trusted providers

1.

(b) ensure the protection of the essential security interests of the Union and each of its Member States, ensuring in particular the national security of each Member State is not prejudiced.

Commented [A81]: The application of Article 12(5) in selecting providers for the Reserve may be prejudicial to Ireland's national security.

Article 17

Support to third countries

1. A DEP-associated third country, in respect of part or all of their territories, may request support from the EU Cybersecurity Reserve where the agreement, or Association Council decision through which it is associated to DEP provides for participation in the Reserve.

Commented [A82]: This could be applicable to Northern Ireland if the UK chose to have an association agreement with the DEP.

2. Support from the EU Cybersecurity Reserve shall be in accordance with this Regulation, shall be approved by the Council, and shall comply with any specific conditions laid down in the agreement, or decision referred to in paragraph 1.

Commented [A83]: We are flexible where this appears in the text but we share the views epxressed by many MS that any deployment to third countries needs to be approved by the Council.

FRANCE

[…]

Whereas:

[…]

(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.

Commented [A84]: FR : proposal to simplify the sentence.

(3) It is necessary to strengthen the european 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[39], it is necessary to increase the resilience of citizens, businesses and entities operating high and other 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 and support in better preparing for, as well as responding to significant and large-scale cybersecurity incidents. ~~Building~~ **With respect to** ~~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.

Commented [A85]: FR : proposal to specify that one of the objective is to strengthen the EU competitiveness

Commented [A86]: FR : proposal to be in accordance with the recital 2

Commented [A87]: FR : the wording « building on » might create confusion and lead to leverage through a new structure activities that are already conducted within the CSIRT network. Proposal to withdraw building.

[39] 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[40], Commission Recommendation (EU) 2017/1584[41], Directive 2013/40/EU of the European Parliament and of the Council[42] and Regulation (EU) 2019/881 of the European Parliament and of the Council[43]. 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.

Commented [A88]: FR : to be in compliance with NIS2, should not we refer to essential and important entities instead of critical infrastructures ?

(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 empower existing infrastructure such as the CSIRT Network to respond to cybersecurity threats and incidents. Member States have also invited the Commission to present a proposal on a new Emergency Response Fund for Cybersecurity in the Council Conclusions on an EU Cyber Posture[44].

Commented [A89]: FR : the response to cyber threats and incidents is the role of the CSIRT network
If the « SOC platform » aims to empower the CSIRT network, then it will contribute to strengthen the CSIRT network capacity to respond to cyber incidents and face cyber threats

---

40 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).

41 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).

42 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).*

43 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).

44 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[45] adopted on 10 November 2022 announced an EU Cyber Solidarity Initiative with the following objectives: strengthening ~~of common~~ EU detection, situational awareness and empowering response capabilities by promoting the ~~deployment~~ establishment of an EU ~~infrastructure of Security Operations Centres ('SOCs')~~support platform, supporting gradual ~~building~~ establishment 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 cybersecurity incidents, with respect to the existing structures and in close cooperation with them. Therefore a pan-European ~~infrastructure of SOCs~~ support platform (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 structures such as the CSIRT network** ~~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**, with due respect** ~~for of~~ **Member State competences and without duplication of the activities conducted by the CSIRT network, EU-CyCLONe and the NIS Cooperation Group**. These actions shall be without prejudice to Articles 107 and 108 of the Treaty on the Functioning of the European Union ('TFEU').

Commented [A90]: FR : proposal to be aligned with the new proposal dealing with « coordinated » EU detection instead of common detection.

Commented [A91]: FR : proposal to be aligned with the new proposal aiming to deal with the enhancement of the CSIRT network capabilities.

Commented [A92]: FR : proposal that are in line with NL proposals

Commented [A93]: FR : the SOC platform is a « support platform » and the legislative proposal should refer to it as it is. Following DE/CZ/NL/DK/PL comments, the « SOC platform » is an information sharing channel and should be defined as such.

Commented [A94]: FR : this sentence is confusing. Proposal of clarification

Formatted: Font: (Default) +Headings CS (Times New Roman), Not Bold, No underline

Commented [A95]: FR ; proposal in line with recital 2.

Commented [A96]: FR : proposal in line with NL comments

Commented [A97]: FR : proposal to specify that the coordinated detection capabilities will empower the CSIRT network.

[45] 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[46] 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 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. This will be complemented by the specific conditions under which financial support may be granted for those actions should be established and the governance and coordination mechanisms necessary in order to achieve the intended objectives should be defined. Other amendments to Regulation (EU) 2021/694 should include descriptions of proposed actions under the new operational objectives, as well as measurable indicators to monitor the implementation of these new operational objectives.

Commented [A98]: FR : proposal to specify that it is also an objective of cooperation / coordination on cybersecurity.

[…]

(12) To more effectively prevent, assess and respond to cyber threats and incidents, it is necessary to develop more comprehensive knowledge about the threats to critical assets and infrastructures on the territory of the Union, including their geographical distribution, interconnection and potential effects in case of cyber-attacks affecting those infrastructures. A large-scale Union ~~infrastructure of SOCs~~ support platform should be ~~deployed~~ established ('the European Cyber**security** ~~Shield~~ **Alert System**'), comprising of several interoperating cross-border platforms, each grouping together several National hub entities~~SOCs~~. That infrastructure should serve national and Union cybersecurity interests and needs, leveraging state of the art technology for advanced data collection and analytics tools, enhancing 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[47].

Commented [A99]: FR : proposal in line with NL proposal

Commented [A100]: FR : proposal to deal with national hub entities instead of SOC in order to avoid confusion.
There are 27 definitions of SOC and it might create also confusion to the public and especially the industry.
It would be beneficial to use a neutral wording.

Commented [A101]: FR ; proposal in line with previous recitals.

---

[46] 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).

[47] 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

(13) **Participation in the European ~~Cyber Shield~~ Cybersecurity Alert System should be voluntary for Member States.** Each Member State **that decides to join the European ~~Cyber Shield~~ Cybersecurity Alert System** should designate a **National ~~SOC~~ hub** entity~~public body at national level tasked with coordinating cyber threat detection activities in that Member State.~~ These National ~~SOCs~~ **hub~~s~~** entities should **have ~~act~~** as **functionalities the capacity to act as** a reference point and gateway at national level for participation in the European ~~Cyber Shield~~ **Cybersecurity Alert System** and should **be capable of detecting, aggregating and analysing data relevant to cyber threats and incidents, by using in particular state-of-the-art technologies**. The Cybersecurity Alert System should enhance the CSIRT network ~~and that would be~~by **shar**ing relevant information~~ed appropriately with the CSIRT network~~ **in order to support the network 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 or existing national platforms to conduct the functions of National ~~SOC~~ hub** entity**, 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** entities**.**

(14) As part of the European Cyber**security Alert System** ~~Shield~~, a number of Cross-border Cybersecurity ~~Operations Centres~~ Support platforms ('Cross-border Support platforms ~~SOCs~~') should be established. These should bring together National hub entities ~~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 Support platforms ~~SOCs~~ should be to strengthen capacities to analyse, prevent and detect cybersecurity threats and to support the production of high-quality intelligence on cybersecurity threats, notably through the sharing of **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.

Commented [A102]: FR : proposal in line with the above recitals fostering synergies between the Support Platform and the CSIRT network

Commented [A103]: FR : would it be possible to clarify if it is a reference to national hub entities ?

(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).

(14a) **A Member State selected by the European Cybersecurity Competence Centre (ECCC) following a call for expression of interest to set up a National ~~SOC~~ Hub entity or enhance the capabilities of an existing one, should jointly purchase relevant tools and infrastructures with the ECCC. Such a Member State should be eligible to receive a grant to operate the tools and infrastructures. 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 collaboration ~~SOC~~ Support Platform or enhance the capabilities of an existing one, should jointly purchase relevant tools and infrastructures with the ECCC. Such a Hosting Consortium should be eligible to receive a grant to operate the tools and infrastructures. 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 procurement procedure to purchase the relevant tools and infrastructures should be carried out jointly by the ECCC and relevant contracting authorities from the Member States selected following these calls for expressions of interest. Private entities should therefore not be eligible to participate in the calls for expression of interest to jointly purchase tools and infrastructures with the ECCC, or to receive grants to operate those tools and infrastructures. However, the Member States should have the possibility to involve private entities in the setting up, enhancement and operation of their National ~~SOC~~ Hub entities ~~s~~ and Cross-border ~~SOCs~~ Support Platforms in other ways which they deem appropriate, in compliance with national and Union law. For providing support to National Hub entities, private entities should be eligible to european fundings following processes defined by National cybersecurity coordination center established by the Regulation (EU) 2021/887.**

(15) ~~At national level, the monitoring, detection and analysis of cyber threats is typically ensured by SOCs of public and private entities, in combination with CSIRTs. In addition,~~ CSIRTs exchange information in the context of the CSIRT network, in accordance with Directive (EU) 2022/2555. The Cross-border ~~SOCs~~ Support platform should constitute a new capability that is complementary to the CSIRTs network and that will empower the latter. The Cross-border support platform ~~and~~ **should coordinate and ~~will~~ cooperate closely with it,** by pooling **data** and sharing **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.

Commented [A104]: FR : as FR understands, the joint purchase is between the parties of the consortium and the funding are made available by the ECCC.
Would it be possible to explain if we deal with a joint purchase between the ECCC and the National Hub entity.

Commented [A105]: FR : proposal to clarify the articulation foreseen between between National hub entities and NCCs as NCCs are entities in charge of structuring the national community (please see Regulation EU 2021/887).

Commented [A106]: FR : please see comment above. proposal in line with the proposal to avoid dealing with the wording SOC.

Commented [A107]: FR considers that cooperation and coordination should be foreseen between the CSIRT network and the support platform in order to effectively contribute to the enhancement of the CSIRT network activities.

(16) The Cross-border Support platforms ~~SOC~~s 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 stakeolders ~~actors~~ such as ~~(e.g.,~~ Computer Emergency Response Teams ('CERTs'), CSIRTs, Information Sharing and Analysis Centers ('ISACs'), operators of critical infrastructures~~)~~. The information exchanged among participants in a Cross-border Support platform ~~SOC~~ should be defined between the parties of the consortium and could include data that do not go beyond national defense and security interests (e.g ~~from~~ networks and sensors, threat intelligence feeds, ~~indicators of compromise~~, and contextualised information about incidents, threats and ~~vulnerabilities~~. In addition, Cross-border Support platform ~~SOCs~~ should also enter into cooperation agreements with other Cross-border Support platform ~~SOCs~~.

(17) Shared situational awareness among relevant authorities is an indispensable prerequisite for Union-wide preparedness and coordination with regards to significant and large-scale cybersecurity incidents. Directive (EU) 2022/2555 establishes the EU–CyCLONe to support the coordinated management of large-scale cybersecurity incidents and crises at operational level and to ensure the regular exchange of relevant information among Member States and Union institutions, bodies and agencies. 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 Support Platforms obtain information related to a potential or ongoing large-scale cybersecurity incident, they should provide relevant information to the CSIRTs network.

~~Recommendation (EU) 2017/1584 on coordinated response to large-scale cybersecurity incidents and crises addresses the role of all relevant actors. Directive (EU) 2022/2555 also recalls the Commission's responsibilities in the Union Civil Protection Mechanism ('UCPM') established by Decision 1313/2013/EU of the European Parliament and of the Council, as well as for providing analytical reports for the Integrated Political Crisis Response Mechanism ('IPCR') arrangements under Implementing Decision (EU) 2018/1993. Therefore, in situations where Cross-border SOCs obtain information related to a potential or ongoing large-scale cybersecurity incident, they should provide relevant information to EU-CyCLONe, the CSIRTs network and the Commission. In particular, depending on the situation, information to be shared could include technical information, information about the nature and motives of the attacker or potential attacker, and higher-level non-technical information about a potential or ongoing large-scale cybersecurity incident.~~ In this context, due regard should be paid to the need-to-know principle and to the potentially sensitive

Commented [A108]: FR ; proposal to deal with stakeholders instead of actors

Commented [A109]: FR :outlines that it should not concerned security and defense information

Commented [A110]: FR recalls that it is already done within the CSIRT network.
See article 15 of NIS2

Commented [A111]: FR recalls that it is a competence of the CSIRT network (please see article 15 of NIS2)

Commented [A112]: FR : as already mentionned in previous comments, the EC is part of CyCLONe and would have access to the information through CyCLONe.
FR would really appreciate to be provided with further information on the need to add up the EC in this part.

nature of the information shared. In accordance with Directive (EU) 2022/2555 the CSIRTs network will, if relevant, inform EU-CyCLONe on the basis of their agreed procedural arrangements for cooperation. As EU-CyCLONe consists of the representatives of Member States' cyber crisis management authorities as well as, in cases where a potential or ongoing large-scale cybersecurity incident has or is likely to have a significant impact on services and activities falling within the scope of this Directive, the information from a Cross-border Support Platform will be distributed through the existing cybercrisismanagement structures in the Union. The Commission will be appropriately informed as an observer / member of EU-CyCLONe.

(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**~~ cause**s** ~~**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 should be able to issue guidance in this respect in close coordination with the ECCC, and with respect to national defense 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, **correlating,** sharing and exchanging **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 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**

Commented [A113]: FR : proposal in line with the Danish proposal to avoid duplication between the CSIRT network and the Support platform

Commented [A114]: FR : typo proposal

Commented [A115]: FR : would it be possible to be provided more information on what it entails

Commented [A116]: FR : the development of tools might fall within the scope of investing / funding in relevant key technologies (role of the ECCC)
More, it should be done with due respect of national defense and security interests.

Formatted: Font: (Default) +Headings CS (Times New Roman), Not Highlight

System with the pan-European High Performance Computing infrastructure established by Council Regulation (EU) 2021/1173[48].

(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 'High Representative'), should gradually develop dedicated protocols and standards to allow for cooperation with the cyber defence community, including vetting and security conditions.~~ The development of the European Cyber**security Alert System** ~~Shield~~ ~~c~~should be accompanied with ~~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 stoke of the developments foreseen for the cooperation between the CSIRT network and the Military CERT network.

(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.

~~**(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.**~~

Commented [A117]: FR considers that the establishment of the Cross border support platform should be on a step by step basis. Cooperation is first foreseen between the CSIRT network and the MICNET > on the basis of the council proposal for a cyber defense policy.
The cooperation with the defense community should be based on this future cooperation.

See our suggestion amendment in this regards.

Commented [A118]: FR : would it be possible to be provided with further clarifications on the processes to be followed regarding the sensitive data that are not classified ?
Will there be a Traffic light protocol put in place ?
What about the sharing of classified information ? Which kind of channel will be used ?

One option could be to align those issues with disposition of directive 2022/2555 NIS2.

[48] 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).

(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 cybersecurity incidents and complement Member States' actions through emergency financial support for preparedness, response and **initial** ~~**immediate**~~ recovery of essential services. The initial recovery encompasses XXXX. 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').

Commented [A119]: FR : it might be useful to explain what initial recovery covers.
This notion would benefit from a definition or specification in the recital part.
FR will come back with a proposal.

Formatted: Font: (Default) +Headings CS (Times New Roman), Highlight

(25) The Cyber Emergency Mechanism should provide support to Member States complementing their own measures and resources, and other existing support options in case of response to and ~~**immediate**~~ **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[49] ~~**and Hybrid Rapid Response Teams**~~. It should address the need to ensure that specialised means are available to support preparedness and response to cybersecurity incidents across the Union and in third countries.

Commented [A120]: FR : same comment than above on the « initial recovery »

(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**~~[50], **the EU Integrated Political Crisis Response Arrangements under Council Implementing Decision (EU) 2018/1993**~~**IPCR**~~[51] **(IPCR Arrangements),**

---

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

50 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).

51 **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.~~

Commission Recommendation 2017/1584[52] 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. 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 ENISA and the affected Member State should be ensured. When requesting support under the Cyber Emergency Mechanism, the Member State should provide relevant information justifying the need for support.

Commented [A121]: FR : if ENISA is in charge of the reserve and then the cooperation should also be foreseen between ENISA and Member states

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

[52] **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).**

(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. For this purpose, the Commission, with the support of ENISA and in cooperation with 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[53]. 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.

Commented [A122]: FR : underlines that EU CyCLONe is a cyber crisis management network and would be suitable to assess the sectors that are the most targeted and vulnerable.

(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**. 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

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

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

(33) A Union-level Cybersecurity Reserve should gradually be set up, consisting of services from **trusted** private providers of managed security services to support response and ~~**immediate**~~ **initiate** recovery actions in cases of significant or large-scale cybersecurity incidents. The EU Cybersecurity Reserve should ensure the availability and readiness of services. The services from the EU Cybersecurity Reserve should serve to support national authorities in providing assistance to affected entities operating in **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, users of the reserve identified as Member States or EUIBAS or Third countries associated to DEP should specify the support provided to the affected entity at the national level, which should be taken into account when assessing the ~~Member State~~users request. The meaning of significant or large scale incidents affecting entities operating in sectors of high criticality or other critical sectors for third countries sould be aligned with article XX od Directive 2022/2555. Associated third countries should be entitled to request the service from the EU Cybersecurity Reserve when the entities targeted and for those they request the EU Cybersecurity reserve, are those operating in the sectors referred in the Annex I and II of Directive 2022/2555 and when the cybersecurity incidents detected lead to an operational overrun or might have spill over effects in the EU.

5 **The CSIRT Network and EU CyCLONe established in Directive EU 2022/2555 can ~~can~~ advise the Commission in reviewing requests for support from the EU Cybersecurity Reserve. EU-CyCLONe should also be informed about requests of assistance.** The services from the EU Cybersecurity Reserve may also serve to support Union institutions, bodies and agencies, under similar conditions. If the request comes from a third country, the Council should be involved in the assessment of the request.

Formatted: Manual Considérant

Commented [A123]: FR : would it be possible to specify to whom do you refer to : ENISA ? COM ? the Service providers ?

Commented [A124]: FR : it clarifies the article 12 and 13 of the text

Commented [A125]: FR : CyCLONe has a key role to play in establishing a situational overview of incidents and it would be logical for CyCLONe to be informed about the latest developments.

Commented [A126]: FR considers there is a need to have two types of procedure for EUMS and Third countries, with the relevant instances involved.

(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, ENISA may be the contracting authority for those services with whose operation and administration it has been entrusted. The procurement procedures to establish the EU Cybersecurity Reserve should be conducted in accordance with Regulation EU 2018/1046. 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 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. 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.

Commented [A127]: FR : it would be beneficial for MS to be informed about the specific information that will be covered by the framework contract.

Commented [A128]: FR : France would like to introduce a scrutiny reserve to explore the legal aspects.

(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 ~~implementation o~~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 Cyber 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 NIS Cooperation Group, the Commission should ensure that the views of Member States as regards priorities and evolution of the EU Cybersecurity Reserve are taken into account.

Commented [A129]: FR : proposal to clarify when the Member states should be involved.

(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.

(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, and the CSIRTs network or the Commission**, with due respect of Member states competences,** 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. The Commission should ~~promptly~~ inform EU-CyCLONe and the CSIRT network about the ~~reasons of~~ the request to ENISA. After the completion of a review and assessment of an incident, ENISA should prepare an incident review report, in collaboration with relevant stakeholders, including representatives from the private sector, Member States, the Commission and other relevant EU institutions, bodies and agencies. As regards the private sector, ENISA is developing channels for exchanging information with specialised providers, including providers of managed security solutions and vendors, in order to contribute to ENISA's mission of achieving a high common level of cybersecurity across the Union. Building on the collaboration with stakeholders, including the private sector, the review report on specific incidents should aim at assessing the causes, impacts and mitigations of an incident, after it has occurred. Particular attention should be paid to the input and lessons shared by the managed security service providers that fulfil the conditions of highest professional integrity, impartiality and requisite technical expertise as required by this Regulation. The report should be delivered and feed into the work of the EU=-CyCLONe, the CSIRTs network and the Commission. When the incident relates to a third country, it **should** ~~will~~ also be shared by the Commission with the High Representative.

Commented [A130]: FR : new proposal to ensure that the information requested by the COM can not be provided by EU CyCLONe / CSIRT network

(37) Taking into account the unpredictable nature of cybersecurity attacks and the fact that they are often not contained in a specific geographical area and pose high risk of spill-over, the strengthening of resilience of neighbouring countries and their capacity to respond

effectively to significant and large-scale cybersecurity incidents contributes to the protection of the Union as a whole. Therefore, third countries associated to the DEP may be supported from the EU Cybersecurity Reserve, where this is provided for in the **~~respective association~~ relevant** agreement **or Association Council decision through which ~~to~~ the third country is associated** to DEP. **The CSIRT Network established in Directive EU 2022/2555 can advise the Commission in reviewing requests for support from the EU Cybersecurity Reserve.** 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**~~.

Commented [A131]: FR : would it be possible to be provided with the analysis of the legal service of the Council to know the legal consequences of the wording changes.
Does it broaden the scope of third countries concerned ?

(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.

[…]

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 ~~Security Operations Centres~~Support platforms ('European ~~Cyber Shield~~ **Cybersecurity Alert System**') to build and enhance ~~common~~ coordinated detection and common situational awareness capabilities, with respect of the competences of existing infrastructures;

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

(c) the establishment of a European Cybersecurity Incident Review Mechanism to review and assess the process of responding to significant or large-scale incidents, with due respect of the Member states competences and in particular, the activities conducted by the CSIRT network, EU-CyCLONe and the NIS Cooperation group.

2. This Regulation pursues the objective to strengthen solidarity at Union level **and enhance Member States cyber resilience** through **the** following specific objectives:

(a) to strengthen ~~common~~ 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, defined by the Annex I and II of the Directive (EU) 2022/2555, across the Union and strengthen solidarity by developing **enhanced** ~~common~~ response capacities **to handle** ~~against~~ significant or large-scale cybersecurity incidents, including by making Union cybersecurity incident response support available for third countries associated to the Digital Europe Programme ('DEP');

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

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

Commented [A132]: FR : proposal to be consistent with the proposed changes in the recitals.
The use of « deployment » might create confusion with the use of « deployment » of the cyber reserve.

Commented [A133]: FR : proposal to be in line with the changes proposed in the recital 7 of the REV2

Commented [A134]: FR : proposal to be in line with the changes proposed in the recital 2 of the REV2.

Commented [A135]: FR : suggestions to define what « initial recovery » means.

Commented [A136]: FR : in line with NL proposal to clarify that the assessment should correspond to the « process of responding to large scale cyber incidents »

Commented [A137]: FR : proposals to be consistent with the changes incorporated in the article 18 on the incident review mechanism

Commented [A138]: FR : please see comment on the article 1. 1. a

Commented [A139]: FR : even if it is already mentionned in the definitions part, we would suggest to specify that sector of « high criticality » and other critical sectors are those mentionned in NIS2

4. **Without prejudice to Article 346 TFEU, the 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 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.**

Article 2

Definitions

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

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

(a) **it has the capacity to act as a reference point and gateway to other public and private organisations at national level for collecting and analysing ~~information~~ on cyber threats and incidents and could contribut~~eing~~ to a Cross-border support ~~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;**

(c) The national hub entity could be a CSIRT designated or established pursuant to Article 10 of Directive (EU) 2022/2555.

(1) '**Cross-border Security Operations Centre ~~collaboration~~ Support Platform' ("Cross-border ~~SOC~~ support collaboration Platform**") means a multi-country platform, **established by a written consortium agreeement** that brings together in a coordinated network structure **N~~n~~**ational ~~SOC~~**s Hubs** entities from at least three Member States ~~who form a Hosting Consortium~~, and that is designed to enhance the **monitoring, detection and analysing of e** ~~prevent~~ cyber threats ~~and~~ **to prevent** incidents and to support the production of **cyber threat** ~~high-quality~~ intelligence, notably through the exchange of **information ~~data~~** ~~from various sources, public and private~~, as well as through the sharing of state-of-the-art tools and jointly

Commented [A140]: FR : it would also be relevant to specify that for non classified information, a Traffic light protocol should be followed.

Formatted: Indent: Left: 0 cm, First line: 0 cm

Commented [A141]: FR : please see comments in the recitals.
We suggest to avoid dealing with SOC as it could create confusion. There are 27 definitions of SOC at the EU level. It might be relevant to use a neutral word such as « entity ».

Commented [A142]: FR : please see comment above on the use of the wording SOC
Support to the DE, NL, PL, CZ, DK positions in this regard.
It could be « support platform » or « CTI platform ».

Formatted: Default, Indent: Left: 1 cm, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: Font: (Default) +Headings CS (Times New Roman), 12 pt, English (United States)

Formatted: Font: (Default) +Headings CS (Times New Roman), 12 pt, Font color: Black, English (United States)

Commented [A143]: FR : proposal to specify that the Support platform should be put in place to enhance the monitoring, detection and analysing of cyber threats.
As it contributes to this enhnacement, then it supports the empowerement of the CSIRT network

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[54];~~

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

Commented [A144]: FR : it could be also « CTI platform »

(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;

(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;

~~(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;~~

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

~~(11)~~ **(8a)** **'trusted providers'** means managed security service providers as defined in Article 6, point (40), of Directive (EU) 2022/2555 selected in accordance with Article 16 of this Regulation.

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

Chapter II

THE EUROPEAN ~~CYBER SHIELD~~ CYBERSECURITY ALERT SYSTEM

Article 3

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

1. An interconnected pan-European infrastructure **that consists** of **National ~~SOC~~ hub entities and Cross-border ~~SOC~~ support collaboration platforms joining on a voluntary basis** ~~Security Operations Centres ('European Cyber Shield~~ **the European Cybersecurity Alert System**~~')~~ shall be established to **support the** develop**ment of** advanced capabilities for the Union to enhance detection, analysis~~e~~ and data processes capabilities ~~data~~ on cyber threats and incidents in the Union. ~~It shall consist of all National Security Operations Centres ('National SOCs') and Cross-border Security Operations Centres ('Cross-border SOCs').~~

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

2. With due respect of the competences of activities conducted by existing infrastructures such as the CSIRT network, t~~T~~he European ~~Cyber Shield~~ **Cybersecurity Alert System** shall:

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

   (b) **share** ~~**produce**~~ high-quality, actionable information and cyber threat intelligence, through the use of state-of-the art tools **and advanced technologies such as**~~, notably A~~artificial ~~I~~intelligence 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** empowering, **supporting and cooperating with relevant entities such as competent**

Commented [A145]: FR : as already mentionned by DK, « interconnected » should be clearly defined. For example, it could be a definition in the definition part (article 2) ;
If it is not defined, then we would suggest to withdraw the word « interconnected » as it might create confusion on « what » will interconnected.

➢Do we refer to all National hub entities ? or do we refer to the platform only ?
➢Will it be shaped as a network ? If so, it might create more confusion and duplication of efforts with the activities of the CSIRT network.

Commented [A146]: FR : or « CTI platform » as suggested by NL

Commented [A147]: FR : wording proposal to clarify what it entails.

Commented [A148]: FR : proposal in order to be consistent with amendments incorporated in the recital 2 of the REV2.

Commented [A149]: FR : or « CTI platform »

Commented [A150]: FR : suggestion to define what « actionable » information means and the purpose ?
Usually an information is already actionable compared to data that need analysis

Commented [A151]: FR : proposal to be consistent with recital 2

authorities designated or established pursuant to Article 8 of Directive (EU) 2022/2555, CSIRTs and the CSIRTs network;

(d) contribute to **enhance**~~d~~ ~~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 ~~Security Operations Centres~~ Hub entities ~~s~~

1. ~~In order~~ **Where a Member State decides** to **voluntarily** participate in the European ~~Cyber Shield~~ **Cybersecurity Alert System**, ~~each Member State~~ **it** shall designate at least one National SOC **Hub**. ~~The National SOC shall be a public body.~~

   ~~It shall have the capacity to act as a reference point and gateway to other public and private organisations at national level for collecting and analysing information on cybersecurity threats and incidents and contributing to a Cross-border SOC. It shall be equipped with state-of-the-art technologies capable of detecting, aggregating, and analysing data relevant to cybersecurity threats and incidents.~~

2. Following a call for expression of interest, **Member States intending to participate in the European ~~Cyber Shield~~ Cybersecurity Alert System** ~~National SOCs~~ shall be selected by the European Cybersecurity Competence Centre ('ECCC') to **take part** ~~participate~~ in a joint procurement of tools and infrastructures with the ECCC**, in order to set up National ~~SOC~~ hub entities or enhance and empower 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

Commented [A152]: FR : typo

Commented [A153]: FR : proposal to be consistent with recital 7

Commented [A154]: FR would recommend to clarify in the disposition who will be in charge to issue these alerts to relevant entities.
We would prefer to keep it flexible and not mention it.

the remaining costs to be covered by the Member State. Before launching the procedure for the acquisition of the tools and infrastructures, the ECCC and the **Member State** ~~National SOC~~ shall conclude a hosting and usage agreement regulating the usage of the tools and infrastructures.

3. A **Member State** ~~National SOC~~ selected pursuant to paragraph 2 shall commit to apply **for their National** ~~SOC~~ **hub** entities~~s~~ to participate in a Cross-border ~~SOC~~ support **collaboration Platform** within two years from the date on which the tools and infrastructures are acquired, or on which it receives grant funding, whichever occurs sooner. If a **Member State's** National ~~SOC~~ **hub** entity is not a participant in a Cross-border ~~SOC~~ support **collaboration Platform** by that time, **the Member State** ~~it~~ shall not be eligible for additional Union support under this **Chapter** ~~Regulation~~.

Commented [A155]: FR suggests to differentiate two different timelines.

Article 5

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

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

Commented [A156]: FR : typo

[…]

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.

4. A Cross-border support ~~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** support ~~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 and infrastructures already jointly procured with that Hosting Consortium.

Article 6

Cooperation and information sharing within and between cross-border ~~SOCs~~ supports collaboration Platforms

1. Members of a Hosting Consortium shall **ensure that their National SOC hubs** exchange**, in accordance with the Consortium Agreement,** relevant information among themselves within the Cross-border SOC **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 foster and enhance the prevention, detection of cyber threats~~,~~ and empower the CSIRT network to respond to or recover from incidents ~~or~~ to mitigate their impact;

   (b) enhances the level of cybersecurity, in particular through raising awareness in relation to cyber threats, limiting or impeding the ability of such threats to spread, supporting a range of defensive capabilities, ~~vulnerability remediation and disclosure~~, threat detection, containment and prevention techniques, mitigation strategies, or response and recovery stages or promoting collaborative threat research between public and private entities.

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

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

   (b) a governance framework **clarifying and** incentivising the sharing of information **referred to in paragraph 1** by all participants;

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

Commented [A157]: FR recalls that it is a competence of the CSIRT network (article 15 of NIS2)

Commented [A158]: FR recalls that it is a competence of the CSIRT network (article 15 of NIS2)

Commented [A159]: FR recalls that it is the competence of the CSIRT network (article 15 of NIS2)

Commented [A160]: FR : same than previous comments Please see suggestion that mentions the empowerement of the CSIRT network thanks to information that could be shared through the Support platform.

This proposal would be in line with article 7

Commented [A161]: FR recalls that it is the role of the CSIRT network (please see article 15 of NIS2)

3. To encourage exchange of information between Cross-border support ~~SOCs~~ **collaboration Platforms**, Cross-border support ~~SOCs~~ **collaboration Platforms** shall ensure a high level of interoperability between themselves. To facilitate the interoperability between the Cross-border ~~SOCs~~ support **collaboration Platforms**, the Commission may, by means of implementing acts**~~, after consulting the ECCC,~~** specify the conditions for this interoperability. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2) of this Regulation. **Before submitting those draft implementing acts to the committee referred to in Article 21(1), the Commission shall consult the ECCC and existing Cross-border SOC collaboration Platforms.**

4. Cross-border SOC~~s~~ **collaboration 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. ~~1.~~ Where a ~~the~~ Cross-border ~~SOCs~~ support **collaboration Platforms** obtain information ~~n~~ relating to a potential or ongoing large-scale cybersecurity incident, they shall **ensure** ~~provide~~ **that** relevant information **is provided** to **the CSIRTs network,** EU-=CyCLONe, ~~the CSIRTs network,~~ ~~and the Commission~~, in view of their respective crisis management roles in accordance with Directive (EU) 2022/2555 without undue delay.

2. Specific coodinnation agreement should be drafted between the Support collaboration Platforms and the CSIRT network in order to ensure that the activities conducted by the Support collaboration Platforms does not duplicate the activities of the CSIRT network.

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

Article 8

Security

1. Member States participating in the European ~~Cyber Shield~~ **Cybersecurity Alert System** shall ensure a high level of data security and physical security of the European ~~Cyber Shield~~ **Cybersecurity Alert System** infrastructure, and shall ensure that the infrastructure ~~shall be~~ **is**

Commented [A162]: FR : would it be possible to be provided with information of which EU level entities do you refer to ? Suggestion to specify what it entails > EUIBAS ?

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.63 cm + Indent at: 1.64 cm

Commented [A163]: FR considers that as the Commissioni part of CyCLONe it will also have access to the information

Commented [A164]: FR : please see proposal to ensure that there is a coordination between the CSIRT network / Support platform and that the activities conducted by the Support platform would not duplicate the efforts.

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 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. Specific security rules should be defined in order to ensure the protection of sensitive non classified information with the respect of traffic light protocols.

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** paragraph**s** 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.

Commented [A165]: FR would suggest to introduce such a disposition to ensure that sensitive information that are not classified are protected as referred to article 10 of directive 2022/2555 :
"As part of such cooperation relationships, Member States shall facilitate effective, efficient and secure information exchange with those third countries' national computer security incident response teams, using relevant information-sharing protocols, including the traffic light protocol."

Commented [A166]: FR supports the DK, CZ, PL, NL remarks.
Should not be the role of the Consortium (parties to the Consortium) to define specific rules / guidance in the contract on how to deal with security aspects ?

Chapter III

CYBER EMERGENCY MECHANISM

Article 9

Establishment of the Cyber Emergency Mechanism

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

[...]

Article 10

Type of actions

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

(a) preparedness actions to be provided by trusted providers for those services would have been certified following the amendment of the Cybersecurity Act (UE 2019/881) ~~:~~ ~~including~~

(vii) the coordinated preparedness testing of entities operating in **sectors of high criticality**, identified by the Annex I of the Directive (EU) 2022/2555 ~~highly critical sectors~~ across the Union;

(viii) **other preparedness actions for entities operating in sectors of high criticality ~~critical~~ and other ~~highly~~ critical sectors, including those involving exercises and trainings and ;**

(b) ~~response~~ actions~~,~~ supporting response to and **initiating** ~~immediate~~ recovery from significant and large-scale cybersecurity incidents, to be provided by trusted providers participating in the EU Cybersecurity Reserve established under Article 12;

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

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

Article 11

Coordinated preparedness testing of entities

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

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

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

Commented [A167]: FR : suggestion to clarify « who » will conduct the preparedness actions ?

Commented [A168]: FR : proposal to include what « coordinated presparedness testing » means.
We would thank the PCY to clarify what is intended under this point.
In our views, this disposition could entail audit on Black box pentest, audit on the information system architecture, audit on the organisational development.

Commented [A169]: FR : suggestion to clarify that we refer to the Directive NIS2

Commented [A170]: FR : as mentionned in the recitals/or definition, it might be useful to explain what « initiating recovery » means.
Would it be possible to be provided with additionnal information from the Commission ?

Commented [A171]: FR : would it be possible to specify which stakeholders are in charge of conducting the coordinated test ? Is it something handled at national level ?
Are MS entitled to funding to fund the coordinated tests ?
Is there a reporting to do after the coordinated test achieved ?
What are the type of coordinated test ?

testing exercises under Article 10 (1) (a) (i). The NIS Cooperation Group, in cooperation 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 12

Establishment of the EU Cybersecurity Reserve

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

2. The EU Cybersecurity Reserve shall consist of incident response services from trusted providers selected in accordance with the criteria laid down in Article 16. During the service provider selection phase, nNational experts should be entitled to participate in the selection process of the trusted service providers as well as - ECCC staff, since it is the ECCC responsibility to manage and monitor the deployment of funds. . The Reserve shall include pre-committed services. The ~~services~~ **Reserve shall** be deployable **upon request** in all Member States **and in third countries referred to in Article 17 (1).**

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

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

   (b) Union institutions, bodies and agencies.

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

4. Users referred to in paragraph 3, point (a), shall use the services **granted upon their request** from the EU Cybersecurity Reserve in order to respond or support response to and **initiate** ~~immediate~~ recovery from significant or large-scale incidents affecting entities operating in **sectors of high** critical**ity** or ~~**highly**~~ **other** critical sectors.

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. Regular updates

Commented [A172]: FR : EU CyCLONe is a cyber crisis management network at the EU level with a key role to play in terms of preparedness.
Those elments could serve the network in its work.

Commented [A173]: FR : proposal to clarify this paragraph as the initial sentence was a bit confused.

Commented [A174]: FR : we consider that it would be essential to define the « initiate recovery » in order to clearly inform the private sector that would apply to the reserve about which kind of actions they would be supposed to conduct.

Commented [A175]: FR : national experts should be entitled to participate in the selection process as it will help to identify specific needs for member states and select appropriate trusted service providers.
This sentence could be moved also to article 16

Also, ECCC is in charge of monitoring DEP projects and we consider key that ECCC be involved in the evaluation process.

Commented [A176]: FR would like to include a scrutiny reserve on this aspect.
A pre-commitment might not lead to an « obligation » but instead an « incentive » of intervention.
We consider important to find the rght balance between attracting the private sector to the reserve and taking into account the possible limited operational capacity available when a large scale cybersecurity incident occurs.

Commented [A177]: FR : it would be useful to provide clarification on the processes for EUIBAS as they are identified as users.
We understood it would also be upon request.
Will it be the Secretariat of the IICB or the CERT EU that will request the assistance ?

Commented [A178]: FR : what about the situation in which the affected entity is located in several member states. Which member state is entitled to request the assistance ?

Commented [A179]: FR : do you refer to third countries competent authorities ? if so, it might be usefull.

Commented [A180]: FR : proposal to clarify the situation for third countries
-High critical sector and other critical sectors are distinguished between the EU and third countries
-Significant or large sclae cybersecurity incidents affecting entities is distinguished between the EU (NIS2 directive definition) and the third countries.

on the contribution agreements should be made available to National competent authorities during CyCLONe Executives meetings.

7. ~~In order to support the Commission in establishing the EU Cybersecurity Reserve,~~ ENISA shall prepare a mapping of the services needed **and their availability**, after consulting ~~**Member States**~~ **the NIS Cooperation Group**, EU CyCLONe and the Commission. ENISA shall prepare a similar mapping, after consulting ~~the~~ **EU CyCLONe, the** Commission **and informing the ~~the~~ NIS Cooperation Group ~~and the~~** ~~Commission~~, to identify the needs of third countries eligible for support from the EU Cybersecurity Reserve pursuant to Article 17. The Commission, where relevant, **may** ~~shall~~ **seek the views of** ~~**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). **Before submitting those drafting implementing acts to the committee referred to in Article 21(1), the Commission may exchange advice and cooperate with** CyCLONe, ~~the~~ **NIS Cooperation Group** and the CSIRT network**.**

Article 13

Requests for support from the EU Cybersecurity Reserve

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

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

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

Commented [A184]: FR : Member states should be informed about the different developments.
EU CyCLONe puts together the 27 national cyber competent authorities and the Commission and ENISA.
It deals with cyber crisis management at EU level and should be informed about the developments on the reserve (especially its constitution).

Commented [A185]: FR : NIS Cooperation group is a « policy » group and EU CyCLONe is an operational network which is suitable for the task.

Commented [A186]: FR : EU CyCLONe is a relevant entity to be consulted about this aspect as it is an operational network dealing with cyber crisis management.
It should be clarify when ENISA would conduct this mapping : is it when there is the assessment of service providers ? is it on month to month basis ? it is upon each request ?

Commented [A187]: FR : please see comment above.

Commented [A188]: FR : proposal to clarify.
-for the operational aspects, CyCLONe should be involved in the process. If there is a large scale cybersecurity incidents and the overrun capacity of several member states, EU Cyclone would probably escalate in warning or full activation mode. It is then logical for the network to be involved.
-for the technical considerations, the CSIRT network should be consulted too.

Commented [A189]: FR : As EU CyCLONe is an operational network dealing with EU cyber crisis management, in case of such large scale cybersecurity incident, it should be informed about a request of assistance (on a voluntary basis as it is a network based on trust and voluntary sharing of information). Indeed, if there is a large scale cybersecurity incidents and the overrun capacity of several member states, EU Cyclone would probably escalate in warning or full activation mode and will be seeking for a comprehensive overview of the situation and actions taken.

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

(a) if possible, appropriate information regarding the affected entity and potential impacts of the incident **on** ~~affected Member State(s) and~~ **users, including the risk of spill over,** and the planned use of the requested support, including an indication of the estimated needs;

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

(c) **where relevant and if possible, available** information about other forms of support available to the affected entity, including contractual arrangements in place for incident response and **initial** ~~immediate~~ recovery services, as well as insurance contracts potentially covering such type of incident.

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

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

[...]

Article 14

Implementation of the support from the EU Cybersecurity Reserve

1. ~~1.~~ Requests for support from the EU Cybersecurity Reserve from users referred to in article 12. 3 point a and b~~,~~ shall be assessed by the Commission, with the support of ENISA or as defined in contribution agreements under Article 12(6), and a response shall be transmitted to the users referred to in Article 12(3) without delay **and in any event no later than 72 hours from the submission of the request to ensure effectiveness of the support action**.

2. EU-CyCLONe and the CSIRT network shall be informed about the request of assistance.

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

[…]

(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).

Commented [A190]: FR : caveat should be included as it should be in compliance with the national security and defense interest clause
For some cyber incidents, it is not possible to share information on the victim as the case might be under a judgment.

Commented [A191]: FR : proposal to keep the sentence simple.

Commented [A192]: FR : we consider EU CyCLONe to be more relevant than the NIS cooperation group, as EU CyCLONe deal with EU cyber crisis management and would better assess which information would be relevant to include in the template.

Commented [A193]: FR : see comment above.

Formatted: Indent: Left: 0 cm, Outline numbered + Level: 7 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 3.81 cm + Indent at: 4.44 cm

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

3. The EU Cybersecurity Reserve services shall be provided in accordance with specific agreements between the service provider and the user to which the support under the EU Cybersecurity Reserve is provided. Those agreements shall include liability conditions.

Commented [A194]: FR would like to put a scrutiny reserve on the legal aspects and will come back later on with comments.

[…]

6. Within **three** ~~one~~ month**s** from the end of the support action, the users shall provide **the** Commission**,** ~~and~~ ENISA**, the CSIRTs network and,** ~~where appropiate,~~ **EU-CyCLONe** with a summary report about the service provided, results achieved and the lessons learned. When the user is from a third country as set out in Article 17, such report shall be shared with the High Representative.

Commented [A195]: FR : EU CyCLONe deals with the EU Cybersecurity crisis management and then the reports will feed its work of preparedness as foreseen under NIS2

7. The Commission shall report to the EU CyCLONe ~~NIS Cooperation Group~~**, on a regular basis and at least once per year,** about the use and the results of the support~~, on a regular basis~~.

Commented [A196]: FR : it should be CyCLONe instead

~~*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[55], the support under this Regulation for responding to such incidents shall complementactions under and without prejudice to Decision 1313/2013/EU.~~

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

~~3. In consultation with the High Representative, support under the Cyber Emergency Mechanism may complement assistance provided in the context of the Common Foreign and Security Policy and Common Security and Defence Policy, including through the Cyber Rapid Response Teams. It may also complement or contribute to assistance provided by one Member State to another Member State in the context of Article 42(7) of the Treaty on the European Union.~~

[55] 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).

4. ~~Support under the Cyber Emergency Mechanism may form part of the joint response between the Union and Member States in situations referred to in Article 222 of the Treaty on the Functioning of the European Union.~~

Article 16

Trusted providers

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

   (a) ensure **that the services included in** the EU Cybersecurity Reserve **are such that the Reserve** ~~includes services that~~ may be deployed in all Member States, taking into account in particular national requirements for the provision of such services, including certification or accreditation;

   […]

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

   […]

   (d) the provider shall have appropriate security clearance, at least for personnel intended for service deployment~~;~~ **, where required by a Member State;**

   […]

   (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.

Commented [A197]: FR : suggest to clarify who will be the contracting authority.

3. Updates on the process followed for the selection of trusted service providers should be made available to the Mangement board of ENISA.

Article 17

Support to DEP-associated third countries

1. **A DEP- associated t**~~T~~hird countr**y**~~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 shall be 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 associated third countries eligible to receive services from the EU Cybersecurity Reserve shall include competent authorities such as CSIRTs and cyber crisis management authorities.

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

5. The Council should be associated to the assessment of the request that comes from third countries. **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**, p~~P~~rior to receiving any support from the EU Cybersecurity Reserve, third countries shall provide to the Commission ~~**and the High Representative**~~ information about their cyber resilience and risk management capabilities, including at least information on national measures taken to prepare for significant or large-scale cybersecurity incidents, as well as information on responsible national entities, including CSIRTs or equivalent entities, their capabilities and the resources allocated to them. **The Commission shall share this information with the Council and the High Representative, for the purpose of facilitating the cooperation referred to in paragraph 6**. Where provisions of Articles 13 and 14 of this Regulation refer to Member States, they shall apply to third countries as set out in paragraph 1.

6. The Commission shall **inform EU CyCLONe,** ~~**the**~~ **NIS Cooperation Group** ~~**Council**~~ **and cooperate**~~coordinate~~ with the High Representative about the requests received and the

Commented [A198]: FR considers that the Council should be involved in the assessment of the request from third countries.

implementation of the support granted to third countries from the EU Cybersecurity Reserve. **The Commission shall take into account the opinions of the NIS Cooperation Group and the High Representative, if such are provided.**

Article 17a) ~~15~~

Coordination with Union crisis management mechanisms

1. **~~In cases w~~Where a significant cybersecurity incident or a large-scale cybersecurity incident~~s~~ originate~~s~~ from or result~~s~~ in a disaster~~s~~ as defined in Article 4, point (1), of Decision No 1313/2013/EU[56], 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~~, 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.**

~~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.~~

Commented [A199]: FR : would like to request for a scrutiny reserve and would come back with additional comments on the text.

~~56 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).~~

Chapter IV

CYBERSECURITY INCIDENT REVIEW MECHANISM

Article 18

Cybersecurity Incident Review Mechanism

1. ~~**After consulting Member States concerned, and A**~~at the request of ~~the Commission~~, the EU-CyCLONe or the CSIRTs network, **and** the Commission **with the agreement of the Member States concerned,** ENISA shall 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 to the CSIRTs network, the EU-CyCLONe and the Commission to support them in carrying out their tasks, in particular in view of those set out in Articles 15 and 16 of Directive (EU) 2022/2555. ~~**Where relevant,**~~ **When an incident has an impact on a third country**, the Commission shall share the report to the Council along with the High Representative.

2. To prepare the incident review report referred to in paragraph 1, ENISA shall collaborate all relevant stakeholders, including representatives of Member States, the Commission, other relevant EU institutions, bodies and agencies, managed security services providers and users of cybersecurity services. Where appropriate, **and ~~in close cooperation~~ with the agreement 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) 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 of the Member State(s) concerned, ENISA may publish** ~~Wwhere possible,~~ a version of the report **containing only public information**. ~~shall be made available~~

Commented [A200]: FR : proposals to be consistent with the recitals and with the CRA.

Commented [A201]: We suggest to referred to the Article 346 TFEU.

~~publicly~~**~~, after consulting Member States concerned.~~** ~~This version shall only include public information.~~

Chapter V

FINAL PROVISIONS

Article 19

Amendments to Regulation (EU) 2021/694

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

(1) Article 6 is amended as follows:

(a) paragraph 1 is amended as follows:

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

'(aa) support the development of an EU ~~Cyber Shield~~ **Cybersecurity Alert System**, including the development, deployment and operation of National and Cross-border SOC~~s~~ **collaboration** platforms that contribute to situational awareness in the Union and to enhancing the cyber threat intelligence capacities of the Union';

[…]

(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.";

[…]

CROATIA

Recitals – terminology consolidation is necessary

Recital 7

Recital 7 is the first recital mentioning "*CSIRT network, EU-CyCLONe and the NIS Cooperation Group*", so we think that in this recital should be added "*established in Directive EU 2022/2555 of the European Parliament and of the Council*[57]". Accordingly, this sentence could be deleted in other recitals (e.g. recital 12 and 33).

Recital 12

Due to changes that has been made in other parts of the Regulation, in recital 12 instead of the term "*National SOCs*" the term "*National SOC Hub*" should be used.

Recital 14

Due to changes that has been made in other parts of the Regulation, in recital 14 (and in any other parts of the Regulation still using this terms) instead of the terms "*Cross-border Cybersecurity Operations Centres ('Cross-border SOCs')*" and "*Cross-border SOCs*", the term "*Cross-border collaboration SOC Platform*" should be used.

Having in mind that "*CSIRT*" has been already mentioned in recital 13, in that recital should be added "*computer incident response team*". This part of the sentence could be deleted in recital 14.

Recital 36

Instead of the term "*providers of managed security solutions*", the term "*providers of managed security services"* should be used.

CHAPTER I

Article 1

We propose to add a new paragraph:

"*3a. The exchange of information under this Regulation shall not entail the supply of information the disclosure of which would be contrary to the essential interests of Member States' national security, public security or defence".*

Article 4

In paragraph 2 singular and plural of the term "*National SOC Hub*" is used. Considering the content of this Paragraph, we think that only singular ("*National SOC Hub*") should be used in it.

CHAPTER II

[57] 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).

Article 7

We propose to add a new sentence at the end of the Paragraph 2:
"The Commission shall exchange advice and cooperate with EU-CyCLONe and CSIRT Network on the draft of those implementing acts."

CHAPTER III

Article 11
We propose to add a new paragraph:
"2a. Member states requests and proposals referred to in Paragraph 1 of this Article shall be transmitted to the Commission via the Member States' cyber crisis management authorities referred to in Article 9 (1) and (2) of Directive (EU) 2022/2555".

Article 12
Having in mind the operational role that EU-CyCLONe has in accordance with Article 16 of NIS2 directive, EU-CyCLONe should be involved in determination of the priorities and evolution of the EU Cybersecurity Reserve, mapping of the services and specifying the types and the number of response services required for the EU Cybersecurity Reserve referred to in Paragraphs 5, 7 and 8 of this Article.
Paragraphs 5, 7 and 8. should be supplemented accordingly:
5.
"To that end, the Commission, in cooperation with the NIS Cooperation Group, EU-CyCLONe and ENISA, shall determine the priorities and evolution of the EU Cybersecurity Reserve ..."
7.
"ENISA shall prepare a mapping of the services needed and their availability, after consulting ~~Member States~~ the NIS Cooperation Group, EU-CyCLONe and the Commission. ENISA shall prepare a similar mapping, after consulting ~~the~~ the NIS Cooperation Group and the Commission, to identify the needs of third countries eligible for support from the EU Cybersecurity Reserve pursuant to Article 17."
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). Before submitting those drafting implementing acts to the committee referred to in Article 21(1), the Commission should exchange advice and cooperate with the NIS Cooperation Group and EU-CyCLONe.

Article 13

Please consider to supplement Paragraph 5 point a) additionally. From the text should be clear that requests for support from users referred to in Article 12(3), points b) and c) should also include relevant information on potential impacts of the incident.

In Paragraph 7 we propose to add a new sentence:

"Before submitting those drafting implementing acts to the committee referred to in Article 21(1), the Commission should exchange advice and cooperate with the NIS Cooperation Group and EU-CyCLONe."

Article 14

In Paragraph 4 should be clearly defined how Member States should be consulted. We think that ENISA should consult NIS Cooperation group on this subject matter.

Taking into account changes that has been made in Recital 33 related to reviewing requests for support from the EU Cybersecurity Reserve, Article 14 should be supplemented also, but instead of CSIRT Network we think that EU-CyCLONe should advise Commission on this subject matter.

New paragraph that should be added:

"1.a The EU-CyCLONe should advise the Commission in reviewing requests for support from the EU Cybersecurity Reserve."

Recital 33 should be adjusted accordingly.

CHAPTER IV

Article 18

Please consider to add additional paragraph which will defined that Member States' cyber crisis management authorities are MS's representatives that is going to be communicated in relation to MS's agreements referred in this Article.

Additional remark in relation to implementing acts – please consider to define in Regulation the deadlines for their adoption.

As general remark - national SOC Hub should be eligible to use the EU funding, regardless of whether MS participates in one of the Cross-Border SOC Platforms.

Regarding the exchange of information, duplication with information exchange activities which are already done within CSIRT network should be avoided. CSoA activities related to the exchange of information should support the exchange of information and cooperation established by the NIS2 Directive.

LATVIA

[…]

Whereas:

[…]

(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[58], it is necessary to increase the resilience of citizens, businesses and entities operating critical infrastructures against the growing cybersecurity threats, which can have devastating societal and economic impacts. Therefore, investment in infrastructures and services that will support faster detection and response to cybersecurity threats and incidents is needed, and Member States need assistance in better preparing for, as well as responding to significant and large-scale cybersecurity incidents. **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.

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

[…]

(7) It is necessary to strengthen the detection and situational awareness of cyber threats and incidents throughout the Union and to strengthen solidarity by enhancing Member States' and the Union's preparedness and capabilities to respond to significant and large-scale cybersecurity incidents. Therefore a pan-European infrastructure of SOCs (European Cyber**security** ~~Shield~~ **Alert System**) should be deployed 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**, with due respect for Member State competences and without duplication of the activities conducted by the CSIRT network, EU-CyCLONe and the NIS Cooperation Group**. These actions shall be without prejudice to Articles 107 and 108 of the Treaty on the Functioning of the European Union ('TFEU').

(8) To achieve these objectives, it is also necessary to amend Regulation (EU) 2021/694 of the European Parliament and of the Council[59] 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 DEP, which aims at guaranteeing the resilience, integrity and trustworthiness of the Digital Single Market, at strengthening capacities to monitor cyber-attacks and threats and to respond to them, and at reinforcing cross-border cooperation on cybersecurity. This will be complemented by the specific conditions under which financial support may be granted for those actions should be established and the governance and coordination mechanisms necessary in order to achieve the intended objectives should be defined. Other amendments to Regulation (EU) 2021/694 should include descriptions of proposed actions under the new operational objectives, as well as measurable indicators to monitor the implementation of these new operational objectives.

[…]

(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

---

59 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).

infrastructures on the territory of the Union, including their geographical distribution, interconnection and potential effects in case of cyber-attacks affecting those infrastructures. A large-scale Union infrastructure of SOCs should be deployed ('the European Cyber**security** ~~Shield~~ **Alert System**'), comprising of several interoperating cross-border platforms, each grouping together several National SOCs. That infrastructure should serve national and Union cybersecurity interests and needs, leveraging state of the art technology for advanced data collection and analytics tools, enhancing cyber detection and management capabilities and providing real-time situational awareness. That infrastructure should serve to increase detection of cybersecurity threats and incidents and thus complement and support Union entities and networks responsible for crisis management in the Union, notably the EU Cyber Crises Liaison Organisation Network ('EU-CyCLONe'), as defined in Directive (EU) 2022/2555 of the European Parliament and of the Council[60].

(13) **Participation in the European ~~Cyber Shield~~ Cybersecurity Alert System should be voluntary for Member States.** Each Member State **that decides to join the European ~~Cyber Shield~~ Cybersecurity Alert System** should designate a **National SOC hub.** ~~public body at national level tasked with coordinating cyber threat detection activities in that Member State.~~ These National SOC~~s~~ **hubs** should **have** ~~act as~~ **functionalities** and **the capacity to act as** a reference point and gateway at national level for participation in the European ~~Cyber Shield~~ **Cybersecurity Alert System** and should **be capable of detecting, aggregating and analysing data relevant to cyber threats and incidents, by using in particular state-of-the-art technologies and that would be shared appropriately with the CSIRT network in order to support the network 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~~may ~~to decide~~ to designate an existing entity such as a CSIRT or ~~existing~~ national platforms 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 Cybersecurity Operations Centres ('Cross-border SOCs') should be established. These

[60] 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).

should bring together National SOCs from at least three Member States, so that the benefits of cross-border threat detection and information sharing and management can be fully achieved. The general objective of Cross-border SOCs should be to strengthen capacities to analyse, prevent and detect cybersecurity threats and to support the production of high-quality intelligence on cybersecurity threats, notably through the sharing of **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.

(14a) A Member State selected by the European Cybersecurity Competence Centre (ECCC) following a call for expression of interest to set up a National SOC Hub or enhance the capabilities of an existing one, should jointly purchase relevant tools and infrastructures with the ECCC. Such a Member State should be eligible to receive a grant to operate the tools and infrastructures. 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 collaboration SOC Platform or enhance the capabilities of an existing one, should jointly purchase relevant tools and infrastructures with the ECCC. Such a Hosting Consortium should be eligible to receive a grant to operate the tools and infrastructures. 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 procurement procedure to purchase the relevant tools and infrastructures should be carried out jointly by the ECCC and relevant contracting authorities from the Member States selected following these calls for expressions of interest. Private entities should therefore not be eligible to participate in the calls for expression of interest to jointly purchase tools and infrastructures with the ECCC, or to receive grants to operate those tools and infrastructures. However, the Member States should have the possibility to involve private entities in the setting up, enhancement and operation of their National SOC Hubs and Cross-border SOCs Platforms in other ways which they deem appropriate, in compliance with national and Union law.

(15) At national level, the monitoring, detection and analysis of cyber threats is typically ensured by SOCs of public and private entities, in combination with CSIRTs. In addition, CSIRTs exchange information in the context of the CSIRT network, in accordance with Directive

(EU) 2022/2555. The Cross-border SOCs should constitute a new capability that is complementary to the CSIRTs network **and will cooperate closely with it,** by pooling **data** and sharing **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.

[…]

(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**~~ cause**s** ~~**and impacts** of cybersecurity~~ **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 should be able to issue guidance in this respect.** This should make it possible to improve collective detection capacities and timely warnings to authorities and relevant entities, notably by using the latest artificial intelligence and data analytics technologies.

(20) By collecting, **correlating,** sharing and exchanging **data and information**, the European ~~Cyber Shield~~ **Cybersecurity Alert System** should enhance the Union's technological sovereignty. The pooling of high-quality curated data should also contribute to the development of advanced artificial intelligence and data analytics technologies. It should be facilitated through the connection of the European ~~Cyber Shield~~ **Cybersecurity Alert System** with the pan-European High Performance Computing infrastructure established by Council Regulation (EU) 2021/1173[61].

(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

[61] 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).

capabilities developed for the protection of critical infrastructure. Cross-border SOCs, with the support of the Commission and the European Cybersecurity Competence Centre ('ECCC'), and in cooperation with the High Representative of the Union for Foreign Affairs and Security Policy (the 'High Representative'), should gradually develop dedicated protocols and standards to allow for cooperation with the cyber defence community, including vetting and security conditions. The development of the European Cyber**security 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.

(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.

~~**(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 cybersecurity incidents and complement Member States' actions through emergency financial support for preparedness, response and **initial ~~immediate~~** recovery of essential services. That instrument should enable the rapid deployment of assistance in defined circumstances and under clear conditions and allow for a careful monitoring and evaluation of how resources have been used. Whilst the primary responsibility for preventing, preparing for and responding to cybersecurity incidents and crises lies with the Member States, the Cyber Emergency Mechanism promotes solidarity between Member States in accordance with Article 3(3) of the Treaty on European Union ('TEU').

(25) The Cyber Emergency Mechanism should provide support to Member States complementing their own measures and resources, and other existing support options in case of response to and **~~immediate~~ 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[62] **~~and Hybrid Rapid Response Teams~~**. It should address the need to ensure that specialised means are available to support preparedness and response to cybersecurity incidents across the Union and in third countries.

(26) This **~~instrument~~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~~**[63], **the EU Integrated Political Crisis Response Arrangements under Council Implementing Decision (EU) 2018/1993~~IPCR~~**[64] **(IPCR Arrangements),**

---

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

63 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).

64 **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.~~

Commission Recommendation 2017/1584[65] 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. 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.

[…]

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

(29) As part of the preparedness actions, to promote a consistent approach and strengthen security across the Union and its internal market, support should be provided for testing and assessing cybersecurity of entities operating in ~~highly critical~~ sectors **of high criticality** identified pursuant to Directive (EU) 2022/2555 in a coordinated manner. For this purpose,

[65] **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).**

the Commission, with the support of ENISA and in cooperation with the NIS Cooperation Group established by Directive (EU) 2022/2555, should regularly identify relevant sectors or subsectors, which should be eligible to receive financial support for coordinated testing at Union level. The sectors or subsectors should be selected from Annex I to Directive (EU) 2022/2555 ('Sectors of High Criticality'). The coordinated testing exercises should be based on common risk scenarios and methodologies. The selection of sectors and development of risk scenarios should take into account relevant Union-wide risk assessments and risk scenarios, including the need to avoid duplication, such as the risk evaluation and risk scenarios called for in the Council conclusions on the development of the European Union's cyber posture ~~to be~~ conducted by the Commission, the High Representative and the NIS Cooperation Group, in coordination with relevant civilian and military bodies and agencies and established networks, including the EU CyCLONe, as well as the risk assessment of communications networks and infrastructures requested by the Joint Ministerial Call of Nevers and conducted by the NIS Cooperation Group, with the support of the Commission and ENISA, and in cooperation with the Body of European Regulators for Electronic Communications (BEREC), the coordinated risk assessments to be conducted under Article 22 of Directive (EU) 2022/2555 and digital operational resilience testing as provided for in Regulation (EU) 2022/2554 of the European Parliament and of the Council[66]. 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**. 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.

[…]

---

66 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

(33) 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 or large-scale cybersecurity incidents. The EU Cybersecurity Reserve should ensure the availability and readiness of services. The services from the EU Cybersecurity Reserve should serve to support national authorities in providing assistance to affected entities operating in **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, Member States should specify the support provided to the affected entity at the national level, which should be taken into account when assessing the Member State request. **The CSIRT Network established in Directive EU 2022/2555 can advise the Commission in 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.

(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, ENISA may be the contracting authority for those services with whose operation and administration it has been entrusted. The procurement procedures to establish the EU Cybersecurity Reserve should be conducted in accordance with Regulation EU 2018/1046. 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 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. 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 in 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 Cyber 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 NIS Cooperation Group, the Commission should ensure that the views of Member States as regards priorities and 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.

(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,** 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 relevant stakeholders, including representatives from the private sector, Member States, the Commission and other relevant EU institutions, bodies and agencies. As regards the private sector, ENISA is developing channels for exchanging information with specialised providers, including providers of managed security solutions and vendors, in order to contribute to ENISA's mission of achieving a high common level of cybersecurity across the Union. Building on the collaboration with stakeholders, including the private sector, the review report on specific incidents should aim at assessing the causes,

impacts and mitigations of an incident, after it has occurred. Particular attention should be paid to the input and lessons shared by the managed security service providers that fulfil the conditions of highest professional integrity, impartiality and requisite technical expertise as required by this Regulation. The report should be delivered and feed into the work of the EU=-CyCLONe, the CSIRTs network and the Commission. When the incident relates to a third country, it **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 as a whole. Therefore, third countries associated to the DEP may be supported from the EU Cybersecurity Reserve, where this is provided for in the ~~respective association~~ **relevant** agreement **or Association Council decision through which ~~to~~ the third country is associated** to DEP. **The CSIRT Network established in Directive EU 2022/2555 can advise the Commission in reviewing requests for support from the EU Cybersecurity Reserve.** 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~~.

(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.

[…]

HAVE ADOPTED THIS REGULATION:

Chapter I

GENERAL OBJECTIVES, SUBJECT MATTER, AND DEFINITIONS

Article 1

Subject-matter and objectives

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

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

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

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

2. This Regulation pursues the objective to strengthen solidarity at Union level **and enhance Member States cyber resilience** through **the** following specific objectives:

   (a) to strengthen common Union detection and situational awareness of cyber threats and incidents thus allowing to reinforce the competitive position of industry and services sectors in the Union across the digital economy and contribute to the Union's technological sovereignty in the area of cybersecurity;

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

   (c) to enhance Union resilience and contribute to effective response by reviewing and assessing significant or large-scale incidents, including drawing lessons learned and,

where appropriate, recommendations **upon request and in coordination with Member States.**

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

Commented [A202]: LV : Insertion of 'sole' in order to align the language with the wording in article 4 (2) of TEU.

4. Without prejudice to Article 346 TFEU, the 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 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.

Article 2

Definitions

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

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

(a) it has the capacity to act as a reference point and gateway to other public and private organisations at national level for collecting and analysing ~~information~~ on cyber threats and incidents and contributing to a Cross-border SOC 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 Security Operations Centre collaboration Platform' ("Cross-border SOC collaboration Platform**") means a multi-country platform, **established by a written consortium agreeement** that brings together in a coordinated network structure **N~~n~~**ational SOC~~s~~ **Hubs** from at least three Member States ~~who form a Hosting Consortium~~, and that is designed to **monitor, detect and analyse** ~~prevent~~ cyber threats ~~and~~ **to prevent** incidents and to support the production of **cyber threat** ~~high-quality~~ intelligence, notably through the exchange of **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[67];~~

(3) **'Hosting Consortium'** means a consortium composed of participating **Member S**~~s~~tates competent authorities, ~~represented by National SOCs,~~ that have agreed to establish and contribute to the acquisition of tools and infrastructure for, and operation of, a Cross-border SOC **collaboration Platform**;

Commented [A203]: LV : Changes made in order to secure that it is not governmental level decision. National SOC hubs could be used.

(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;

(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;

~~(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;~~

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

~~(11)~~ **(8a)** **'trusted providers'** means managed security service providers as defined in Article 6, point (40), of Directive (EU) 2022/2555 selected in accordance with Article 16 of this Regulation.

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

Chapter II

THE EUROPEAN ~~CYBER SHIELD~~ CYBERSECURITY ALERT SYSTEM

Article 3

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

1. An interconnected pan-European infrastructure **that consists** of **National SOC hubs and Cross-border SOC collaboration platforms joining on a voluntary basis** ~~Security Operations Centres ('European Cyber Shield~~ **the European Cybersecurity Alert System**~~')~~ shall be established to **support the** develop**ment of** advanced capabilities for the Union to detect, analyse and process data on cyber threats and incidents in the Union. ~~It shall consist of all National Security Operations Centres ('National SOCs') and Cross-border Security Operations Centres ('Cross-border SOCs').~~

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

2. The European ~~Cyber Shield~~ **Cybersecurity Alert System** shall:

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

   (b) **share** ~~**produce**~~ high-quality, actionable information and cyber threat intelligence, through the use of state-of-the art tools **and advanced technologies such as**~~, notably A~~**a**rtificial ~~I~~**i**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, CSIRTs and the CSIRTs network**;

Commented [A204]: LV : need clarification what the interconnected part means. Does this entail that all National SOC hubs and Cross-border Platforms must be connected?

(d) contribute to **enhanced** ~~faster~~ detection of cyber threats and 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 Security Operations Centres ~~s~~ 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 designate at least one National SOC **Hub**. ~~The National SOC shall be a public body.~~

   ~~It shall have the capacity to act as a reference point and gateway to other public and private organisations at national level for collecting and analysing information on cybersecurity threats and incidents and contributing to a Cross-border SOC. It shall be equipped with state-of-the-art technologies capable of detecting, aggregating, and analysing data relevant to cybersecurity threats and incidents.~~

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

Commented [A205]: LV : selection should be based on defined criteria and those must be identified in the regulation. Our suggestion is use expression of interest from MS to be included in list who take part in procurement.

3. A **Member State** ~~National SOC~~ selected pursuant to paragraph 2 shall commit to apply **for their National SOC hubs** to participate in a Cross-border SOC **collaboration Platform** within two years from the date on which the tools and infrastructures are acquired, or on which it receives grant funding, whichever occurs sooner. If a **Member State's** National SOC **hub** is not a participant in a Cross-border SOC **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 Security Operations Centre~~s~~ collaboration Platforms

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

[…]

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.

4. A 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 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 and infrastructures already jointly procured with that Hosting Consortium.

Article 6

Cooperation and information sharing within and between cross-border SOCs~~s~~ collaboration Platforms

1. Members of a Hosting Consortium shall **ensure that their National SOC hubs** exchange**, in accordance with the Consortium Agreement,** relevant information among themselves within the Cross-border SOC **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:

   […]

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

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

   (b) a governance framework **clarifying and** incentivising the sharing of information **referred to in paragraph 1** by all participants;

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

3. ~~To encourage exchange of information between Cross-border SOCs **collaboration Platforms**, Cross-border SOCs **collaboration Platforms** shall ensure a high level of interoperability between themselves. To facilitate the interoperability between the Cross-border SOCs **collaboration Platforms**, the Commission may, by means of implementing acts, **after consulting the ECCC,** specify the conditions for this interoperability. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2) of this Regulation. **Before submitting those draft implementing acts to the committee referred to in Article 21(1), the Commission shall consult the ECCC and existing Cross-border SOC collaboration Platforms.**~~

   Commented [A206]: LV : cooperation agreement has to be base for colloboration and information exchange.

4. Cross-border SOC~~s~~ **collaboration 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. Where the Cross-border SOC~~s~~ **collaboration Platforms** obtain information relating to a potential or ongoing large-scale cybersecurity incident, they shall **ensure** ~~provide~~ **that** relevant information **is provided** to **the CSIRTs network,** EU-~~=~~CyCLONe, ~~the CSIRTs network,~~ and the Commission, in view of their respective crisis management roles in accordance with Directive (EU) 2022/2555 without undue delay.

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

Commented [A207]: LV: The commitment to share data within the regional SOC consortia should be defined by the participating countries in their respective Consortium Agreements, which allows for a gradual development of the collaboration. Procedural arrangements should be determinet in same Consortium Agreement.

Article 8

Security

1. Member States participating in the European ~~Cyber Shield~~ **Cybersecurity Alert System** shall ensure a high level of data security and physical security of the European ~~Cyber Shield~~ **Cybersecurity Alert System** infrastructure, and shall ensure that the infrastructure ~~shall be~~ **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 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.

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** paragraph**s** 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 and agree with Member States.

Commented [A208]: LV : involvement of MS is important

Chapter III

CYBER EMERGENCY MECHANISM

Article 9

Establishment of the Cyber Emergency Mechanism

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

[…]

Article 10

Type of actions

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

(a) preparedness actions**:**~~,~~ ~~including~~

(ix) the coordinated preparedness testing of entities operating in **sectors of high criticality** ~~highly critical sectors~~ across the Union;

(x) other preparedness actions for entities operating in sectors of high criticality ~~critical~~ and other ~~highly~~ critical sectors, including those involving exercises and trainings and ;

(b) ~~response~~ actions~~,~~ supporting response to and **initiating** ~~immediate~~ recovery from significant and large-scale cybersecurity incidents, to be provided by trusted providers participating in the EU Cybersecurity Reserve established under Article 12;

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

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

Article 11

Coordinated preparedness testing of entities

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

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

2. The NIS Cooperation Group in cooperation with the Commission, ENISA, and the High Representative, shall develop common risk scenarios and methodologies for the **coordinated testing exercises under Article 10 (1) (a) (i). The NIS Cooperation Group, in cooperation with Commission, ENISA and the High Representative, may develop common risk scenarios and methodologies for other preparedness actions under Article 10(1)(a)(ii).**

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, responding or providing support for responding to significant or large-scale cybersecurity incidents, and ~~immediate~~ **initiate** recovery from such incidents.

2. The EU Cybersecurity Reserve shall consist of incident response services from trusted providers selected in accordance with the criteria laid down in Article 16. The Reserve shall include pre-committed services. The ~~services~~ **Reserve shall** be deployable **upon request** in all Member States **and in third countries referred to in Article 17 (1).**

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

   […]

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

4. Users referred to in paragraph 3, point (a), shall use the services **granted upon their request** from the EU Cybersecurity Reserve in order to respond or support response to and **initiate** ~~immediate~~ recovery from significant or large-scale incidents affecting entities operating in **sectors of high** critical**ity** or ~~**highly**~~ **other** critical sectors.

5. The Commission shall ~~responsibility~~ **have overall responsibility** for the implementation of the EU Cybersecurity Reserve. **To that end, the** Commission**, in cooperation with the NIS Cooperation Group and ENISA,** shall determine the priorities and evolution of the EU Cybersecurity Reserve, in line with the requirements of the users referred to in paragraph 3, and shall supervise its implementation, and ensure complementarity, consistency, synergies and links with other support actions under this Regulation as well as other Union actions and programmes. **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 a mapping of the services needed **and their availability**, after consulting ~~**Member States**~~ **the NIS Cooperation Group** and the Commission. ENISA shall prepare a similar mapping, after consulting the **the NIS Cooperation Group and the** Commission, to identify the needs of third countries eligible for support from the EU Cybersecurity Reserve pursuant to Article 17. The Commission, where relevant, **may** ~~shall~~ **seek the views of** ~~**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). **Before submitting those drafting implementing acts to the committee referred to in Article 21(1), the Commission may exchange advice and cooperate with the NIS Cooperation Group.**

Article 13

Requests for support from the EU Cybersecurity Reserve

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

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

[…]

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

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

   (a) appropriate information regarding the affected entity and potential impacts of the incident **on affected Member State(s) and users, including the risk of spill over,** and the planned use of the requested support, including an indication of the estimated needs;

   (b) 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.

[…]

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).

Commented [A209]: LV : regulation should already specify the details, we do not support implementing act.

Article 14

Implementation of the support from the EU Cybersecurity Reserve

1. Requests for support from the EU Cybersecurity Reserve, shall be assessed by the Commission, with the support of ENISA or as defined in contribution agreements under

Article 12(6), and a response shall be transmitted to the users referred to in Article 12(3) without delay **and in any event no later than 72 hours from the submission of the request to ensure effectiveness of the support action**.

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

[…]

(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 and Union institutions, bodies and agencies.

[…]

6. Within **three** ~~one~~ month**s** from the end of the support action, the users shall provide **the** Commission**,** ~~and~~ ENISA**, the CSIRTs network and, where appropiate, EU-CyCLONe** with a summary report about the service provided, results achieved and the lessons learned. When the user is from a third country as set out in Article 17, such report shall be shared with the High Representative.

7. The Commission shall report to the NIS Cooperation Group**, on a regular basis and at least once per year,** about the use and the results of the support~~, on a regular basis~~.

~~*Article 15*~~

~~**Coordination with crisis management mechanisms**~~

~~1. In cases where significant or large-scale cybersecurity incidents originate from or result in disasters as defined in Decision 1313/2013/EU[68], 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.~~

[68] 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.~~

Article 16

Trusted providers

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

   (a) ensure **that the services included in** the EU Cybersecurity Reserve **are such that the Reserve** ~~includes services that~~ may be deployed in all Member States, taking into account in particular national requirements for the provision of such services, including certification or accreditation;

   […]

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

   […]

   (d) the provider shall have appropriate security clearance, at least for personnel intended for service deployment~~;~~ **, where required by a Member State;**

   […]

   (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;

Commented [A210]: LV : Need to take into account that one security clearance won't be applicable to all MS as each country has own procedures, responsible institutions. Need to discuss for possible solution. It needs to be stated who will provide this security clearance. Will a security clearance from a state outside the EU be sufficient ? Will MS be able to deny the use of a provider if they do not have a security clearance from that Member State ?

(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, when it is to be made mandatory through relevant Union law.

Commented [A211]: LV : need to take into account schemes are not mandatory if not decided otherwise.

Article 17

Support to DEP-associated third countries

1. **A DEP- associated t~~T~~hird countr**y**~~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 shall be approved by the Council and 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.

Commented [A212]: LV : Deploying the reserve to a third country is a matter of foreign and security policy, which is a Council prerogative.

[…]

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**, p~~P~~rior to receiving any support from the EU Cybersecurity Reserve, third countries shall provide to the Commission ~~**and the High Representative**~~ information about their cyber resilience and risk management capabilities, including at least information on national measures taken to prepare for significant or large-scale cybersecurity incidents, as well as information on responsible national entities, including CSIRTs or equivalent entities, their capabilities and the resources allocated to them. **The Commission shall share this information with the High Representative, for the purpose of facilitating the cooperation referred to in paragraph 6**. Where provisions of Articles 13 and 14 of this Regulation refer to Member States, they shall apply to third countries as set out in paragraph 1.

6. The Commission shall **inform the NIS Cooperation Group ~~Council~~ and cooperate**~~coordinate~~ with the High Representative about the requests received and the implementation of the support granted to third countries from the EU Cybersecurity Reserve.

The Commission shall take into account the opinions of the NIS Cooperation Group and the High Representative, if such are provided.

Article 17a) ~~15~~

Coordination with Union crisis management mechanisms

1. **~~In cases w~~Where a significant cybersecurity incident or a large-scale cybersecurity incident~~s~~ originate~~s~~ from or result~~s~~ in a disaster~~s~~ as defined in Article 4, point (1), of Decision No 1313/2013/EU[69], 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~~, 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.**

~~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

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

1. ~~**After consulting Member States concerned, and A**~~at the request of the Commission, the EU-CyCLONe or the CSIRTs network, **and with the agreement of the Member States concerned,** ENISA shall review and assess threats, vulnerabilities and mitigation actions with respect to a specific significant or large-scale cybersecurity incident. Following the completion of a review and assessment of an incident, ENISA shall deliver an incident review report to the CSIRTs network, the EU-CyCLONe and the Commission to support them in carrying out their tasks, in particular in view of those set out in Articles 15 and 16 of Directive (EU) 2022/2555. ~~**Where relevant,**~~ **When an incident has an impact on a third country**, the Commission shall share the report with the High Representative.

2. To prepare the incident review report referred to in paragraph 1, ENISA shall collaborate all relevant stakeholders, including representatives of Member States, the Commission, other relevant EU institutions, bodies and agencies, managed security services providers and users of cybersecurity services. Where appropriate, **and ~~in close cooperation~~ with the agreement 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, 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) 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 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 and Cross-border SOC~~s~~ **collaboration** platforms that contribute to situational awareness in the Union and to enhancing the cyber threat intelligence capacities of the Union';

[…]

(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.

[…]

HUNGARY

General comments

HU carefully considered PRES second compromise proposal, recognizing the thoughtful efforts to bridge differences and advance our collective objectives during the written consultation.

We ask PRES to incorporate our position in the proposal along with the opinions of our colleges from like-minded MS groups by **highlighting a simplified procedure as a priority** commit to **fostering consensus and progress in our collaborative endeavours**. **We trust in PRES dedicated efforts** for the work accomplished **striving for clarity and coherence** during future negotiations.

Furthermore, in our understanding, in accordance with the **new recitals (33a) and (33b),** the **COM does not have full contractual responsibility for the implementation of the Reserve**, as it acts as a contracting authority for the establishment, operation and management of the Reserve, and these services **could not be under the responsibility of ENISA**.

Textually, this will be the case, we would appreciate it to know **what practical consequences this amendment will have**. In our views, in order for this above-mentioned mechanism to be effective, it **should be simplified.**

The section does not, however, go into detail on the common rules of liability for damages. Unfortunately, **it only lays down general form of the contract and the specific agreement** to be finalized between the contracting authority and the selected service provider.

Finally, we find it quite essential that all MS is able to participate in a constructive dialogue, offering feedback and insights to refine and enhance the proposal.

NETHERLANDS

[…]

Whereas:

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

(2) The magnitude, frequency and impact of cybersecurity incidents are increasing, including supply chain attacks aiming at cyberespionage, ransomware or disruption. They represent a major threat to the functioning of network and information systems. In view of the fast- evolving threat landscape, the threat of possible large-scale incidents causing significant disruption or damage to critical infrastructures demands heightened preparedness at all levels of the Union's cybersecurity framework. That threat goes beyond Russia's military aggression on Ukraine, and is likely to persist given the multiplicity of state-aligned, criminal and hacktivist actors involved in current geopolitical tensions. Such incidents can impede the provision of public services and the pursuit of economic activities, including in **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[1], it is necessary to increase the resilience of citizens, businesses and entities operating critical infrastructures against the growing cybersecurity threats, which can have devastating societal and economic impacts. Therefore, investment in infrastructures and services that will support faster detection and response to

cybersecurity threats and incidents is needed, and Member States need assistance in better preparing for, as well as responding to and recovering from significant and large-scale cybersecurity incidents. **Building on the existing structures and in close cooperation with them,** ~~T~~the Union should also increase its capacities in these areas, notably as regards the collection and analysis of data on cybersecurity threats and incidents.

---

1 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[1], Commission Recommendation (EU) 2017/1584[2], Directive 2013/40/EU of the European Parliament and of the Council[3] and Regulation (EU) 2019/881 of the European Parliament and of the Council[4]. In addition, the Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure invites Member States to take urgent and effective measures, and to cooperate loyally, efficiently, in solidarity and in a coordinated manner with each other, the Commission and other relevant public authorities as well as the entities concerned, to enhance the resilience of critical infrastructure used to provide essential services in the internal market.

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

---

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

2 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).

3 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).

4 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).

5 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[1] 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 establishment~~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 cybersecurity incidents. Therefore a pan-European infrastructure of SOCs (European Cyber**security ~~Shield~~ Alert System**) should be established~~deployed~~ 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**, with due respect for Member State competences and without duplication of the activities conducted by the CSIRT network, EU-CyCLONe and the NIS Cooperation Group**. These actions shall be without prejudice to Articles 107 and 108 of the Treaty on the Functioning of the European Union ('TFEU').

Commented [A213]: Support.

1 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[1] in certain areas. In particular, this Regulation should amend Regulation (EU) 2021/694 as regards adding new operational objectives related to the European Cyber**security** ~~Shield~~ **Alert System** and the Cyber Emergency Mechanism under Specific Objective 3 of DEP, which aims at guaranteeing the resilience, integrity and trustworthiness of the Digital Single Market, at strengthening capacities to monitor cyber-attacks and threats and to respond to them, and at reinforcing cross-border cooperation on cybersecurity. This will be complemented by the specific conditions under which financial support may be granted for those actions should be established and the governance and coordination mechanisms necessary in order to achieve the intended objectives should be defined. Other amendments to Regulation (EU) 2021/694 should include descriptions of proposed actions under the new operational objectives, as well as measurable indicators to monitor the implementation of these new operational objectives.

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

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

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

(11) For the purpose of sound financial management, specific rules should be laid down for the carry-over of unused commitment and payment appropriations. While respecting the principle that the Union budget is set annually, this Regulation should, on account of the unpredictable, exceptional and specific nature of the cybersecurity landscape, provide for possibilities to carry over unused funds beyond those set out in the Financial Regulation, thus maximising the Cybersecurity Emergency Mechanism's capacity to support Member States in preparing for and countering effectively cyber threats.

(12) To more effectively prevent, assess and respond to cyber threats and incidents, it is necessary to develop more comprehensive knowledge about the threats to critical assets and infrastructures on the territory of the Union, including their geographical distribution, interconnection and potential effects in case of cyber-attacks affecting those infrastructures. A large-scale Union infrastructure of SOCs should be deployed ('the European Cyber**security** ~~Shield~~ **Alert System**'), comprising of several interoperating cross-border platforms, each grouping together several National SOCs. That infrastructure should serve national and Union cybersecurity interests and needs, leveraging state of the art technology for advanced data collection and analytics tools, enhancing cyber detection and management capabilities and providing real-time situational awareness. That infrastructure should serve to increase detection of cybersecurity threats and incidents and thus complement and support Union entities and networks responsible for crisis management in the Union, notably the EU Cyber Crises Liaison Organisation Network ('EU-CyCLONe'), as defined in Directive (EU) 2022/2555 of the European Parliament and of the Council[1].

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

(13) **Participation in the European ~~Cyber Shield~~ Cybersecurity Alert System should be voluntary for Member States.** Each Member State **that decides to join the European ~~Cyber Shield~~ Cybersecurity Alert System** should- appoint the designated CSIRT under Directive 2022/2555 (NIS2), or another public body with a similar mandate, as defined in Article 2(2), that 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 cybersecurity threats and incidents and contributing to a Cross-border collaboration platform, as member of the cross-border collaboration platform.~~designate a National SOC CSIRT hub. public body at national level tasked with coordinating cyber threat detection activities in that Member State.~~ These National SOC~~s~~ **hubs** should **have** ~~act~~ as **functionalities the capacity to act as** a reference point and gateway at national level for participation in the European ~~Cyber Shield~~ **Cybersecurity Alert System** and should **be capable of detecting, ~~aggregating and analysing data~~ relevant to cyber threats and incidents, by using in particular state-of-the-art technologies and that would be shared appropriately with the CSIRT network in order to support the network 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 or existing national platforms 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 Cybersecurity Operations Centres ('Cross-border SOCs') should be established. These should bring together National SOCs from at least three Member States, so that the benefits of cross-border threat detection and information sharing and management can be fully achieved. The general objective of Cross-border SOCs should be to strengthen capacities to analyse, prevent and detect cybersecurity threats and to support the production of high-quality intelligence on cybersecurity threats, notably through the sharing of **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.

Commented [A214]: The Netherlands continues its urge to steer away from the terms 'SOC', taking into account the purpose of this initiative, and using terms that more aptly reflect the objectives of the initiative, such as the term "cross-border platform" as used in the Call for Expression of Interest.

Even more, referring to the designated CSIRT under Directive 2022/2555. will ensure legal consistency in the EU cyber legislation framework.
We hear the Presidency that it should be up to Member States to designate the exact body on a national level. At the same time, it is of the utmost importance to us that we do not introduce any further complexity in our cyber landscape. The NIS2 has been created to harmonise MS approach to cybersecurity, therefore we should also follow this since the projects are linked to the CSIRT Network. So we see a possible compromise with an explicit reference to national CSIRTs in the operative text (as general principle) but with flexibility to designate another public body, with similar functionalities, if deemed necessary by a Member State.

Commented [A215]: Within the Alert System no raw data should be exchanged, but data that is already aggregated/analysed. The Alert System should be about sharing data, not analysing it. Therefore, NL strongly opposes this addition.

Commented [A216]: No support for including this in a recital; this should be arranged within the consortia agreements.

Commented [A217]: No support for this addition since this wording causes to much ambiguity in which kind of entity is eligible as a member of the cross-border SOC platform. NL suggests that only the CSIRTs under Directive 2022/2555 or a public entity with a similar mandate should be eligible. This national CSIRT can act as gateway towards other national entities and platforms.

(14a) A Member State selected by the European Cybersecurity Competence Centre (ECCC) following a call for expression of interest to set up a National SOC Hub or enhance the capabilities of an existing one, should jointly purchase relevant tools and infrastructures with the ECCC. Such a Member State should be eligible to receive a grant to operate the tools and infrastructures. 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 collaboration SOC Platform or enhance the capabilities of an existing one, should jointly purchase relevant tools and infrastructures with the ECCC. Such a Hosting Consortium should be eligible to receive a grant to operate the tools and infrastructures. 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 procurement procedure to purchase the relevant tools and infrastructures should be carried out jointly by the ECCC and relevant contracting authorities from the Member States selected following these calls for expressions of interest. Private entities should therefore not be eligible to participate in the calls for expression of interest to jointly purchase tools and infrastructures with the ECCC, or to receive grants to operate those tools and infrastructures. However, the Member States should have the possibility to involve private entities in the setting up, enhancement and operation of their National SOC Hubs and Cross-border SOCs Platforms in other ways which they deem appropriate, in compliance with national and Union law.

(15) At national level, the monitoring, detection and analysis of cyber threats is typically ensured by SOCs of public and private entities, in combination with CSIRTs. In addition, CSIRTs exchange information in the context of the CSIRT network, in accordance with Directive (EU) 2022/2555. The Cross-border SOCs should constitute a new capability that is complementary to the CSIRTs network **and will cooperate closely with it,** by pooling **data** and sharing **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 SOCs should act as a central point allowing for a broad pooling of relevant data and cyber threat intelligence, enable the spreading of threat information among a large and diverse set of actors (e.g., Computer Emergency Response Teams ('CERTs'), CSIRTs, Information Sharing and Analysis Centers ('ISACs'), operators of critical infrastructures). The information exchanged among participants in a Cross-border SOC could include data from networks and sensors, threat intelligence feeds, indicators of compromise, and contextualised information about incidents, threats and vulnerabilities. In addition, Cross-border SOCs should also enter into cooperation agreements with other Cross-border SOCs.

(17) Shared situational awareness among relevant authorities is an indispensable prerequisite for Union-wide preparedness and coordination with regards to significant and large-scale cybersecurity incidents. Directive (EU) 2022/2555 establishes the EU–CyCLONe to support the coordinated management of large-scale cybersecurity incidents and crises at operational level and to ensure the regular exchange of relevant information among Member States and Union institutions, bodies and agencies. Recommendation (EU) 2017/1584 on coordinated response to large-scale cybersecurity incidents and crises addresses the role of all relevant actors. Directive (EU) 2022/2555 also recalls the Commission's responsibilities in the Union Civil Protection Mechanism ('UCPM') established by Decision 1313/2013/EU of the European Parliament and of the Council, as well as for providing analytical reports for the Integrated Political Crisis Response Mechanism ('IPCR') arrangements under Implementing Decision (EU) 2018/1993. Therefore, in situations where Cross-border SOCs obtain information related to a potential or ongoing large-scale cybersecurity incident, they should provide relevant information to ~~EU CyCLONe,~~ the CSIRTs network ~~and the Commission~~. In accordance with the principles for managing large-scale cybersecurity incidents in Directive (EU) 2022/2555 and their standard operating procedures, the CSIRTs network will notify and share this information with EU CyCLONe if relevant. 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.

Commented [A218]: NL would like to pay attention to coherence with existing structures of EU operational cooperation. In the current governance model, the CSIRT Network has the mandate and technical expertise to determine if certain information is relevant for the EU CyCLONe.

(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~~ cause**s and impacts** ~~of cybersecurity~~ **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 should be able to issue guidance in this respect.** 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.

Commented [A219]: This needs to be clarified, what guidance does the Commission expect to give in this respect?

(20) By collecting, **correlating,** sharing and exchanging **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 also contribute to the development of advanced artificial intelligence and data analytics technologies. It should be facilitated through the connection of the European ~~Cyber Shield~~ **Cybersecurity Alert System** with the pan-European High Performance Computing infrastructure established by Council Regulation (EU) 2021/1173[1].

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

(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 'High Representative'), should gradually develop dedicated protocols and standards to allow for cooperation with the cyber defence community, including vetting and security conditions. The development of the European Cyber**security 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.~~

(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.

(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.**~~

Commented [A220]: This seems to be superfluous and it is too early to anticipate on this in this Act. Also is it questionable whether this is compatible with the legal basis of the proposal.

Commented [A221]: No need to include this in this Act.

(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 cybersecurity incidents and complement Member States' actions through emergency financial support for preparedness, response and ~~initial immediate~~ recovery of essential services. ~~That~~ The Cyber Reserve instrument under the Cyber Emergency Mechanism 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').

Commented [A222]: The preparedness support cannot be classified as 'emergency' financial support since it will often be carried out ex ante. This should be rephrased accordingly.

(25) The Cyber Emergency Mechanism should provide support to Member States complementing their own measures and resources, and other existing support options in case of response to and **~~immediate~~ 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[1] **~~and Hybrid Rapid Response Teams~~**. It should address the need to ensure that specialised means are available to support preparedness and response to cybersecurity incidents across the Union and in third countries.

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

(26) This ~~instrument~~**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~~[1], **the EU Integrated Political Crisis Response Arrangements under Council Implementing Decision (EU) 2018/1993**~~IPCR~~[2] **(IPCR Arrangements),** ~~Commission Recommendation 2017/1584~~[3] 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 PESCO Cyber Rapid Response Teams. 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 ENISA ~~the Commission~~ and the affected Member State should be ensured. When requesting support under the Cyber Emergency Mechanism, the Member State should provide relevant information justifying the need for support.

Commented [A223]: ENISA is the EU Cybersecurity Agency supporting all cooperation networks and the most suited and best equiped organisation to engage with Member States on deployment of the Cyber Reserve, also on the basis of their experience with the current pilot.

---

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

2 **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.~~

~~3~~ ~~**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).**~~

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

Commented [A224]: Suggestion to remove 'immediate / initial' to give more flexibility to recovery services, which includes restoring the functioning of essential services (throughout the text)

(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. For this purpose, the Commission, with the support of ENISA and in cooperation with the NIS Cooperation Group established by Directive (EU) 2022/2555, should regularly identify relevant sectors or subsectors, which should be eligible to receive financial support for coordinated testing at Union level. The sectors or subsectors should be selected from Annex I to Directive (EU) 2022/2555 ('Sectors of High Criticality'). The coordinated testing exercises should be based on common risk scenarios and methodologies. The selection of sectors and development of risk scenarios should take into account relevant Union-wide risk assessments and risk scenarios, including the need to avoid duplication, such as the risk evaluation and risk scenarios called for in the Council conclusions on the development of the European Union's cyber posture ~~to be~~ conducted by the Commission, the High Representative and the NIS Cooperation Group, in coordination with relevant civilian and military bodies and agencies and established networks, including the EU CyCLONe, as well as the risk assessment of communications networks and infrastructures requested by the Joint Ministerial Call of Nevers and conducted by the NIS Cooperation Group, with the support of the Commission

and ENISA, and in cooperation with the Body of European Regulators for Electronic Communications (BEREC), the coordinated risk assessments to be conducted under Article 22 of Directive (EU) 2022/2555 and digital operational resilience testing as provided for in Regulation (EU) 2022/2554 of the European Parliament and of the Council[1]. The selection of sectors should also take into account the Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure.

(30) In addition, the Cyber Emergency Mechanism should offer support for other preparedness actions and support preparedness in other sectors, not covered by the coordinated testing of entities operating in ~~**highly critical**~~ sectors **of high criticality**. 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 assistance provided by Member States to a Member State affected by a significant or large-scale cybersecurity incident, including by the CSIRTs network set out in Article 15 of Directive (EU) 2022/2555. Member States providing assistance should be allowed to submit requests to cover costs related to dispatching of expert teams in the framework of mutual assistance. The eligible costs could include travel, accommodation and daily allowance expenses of cybersecurity experts.

(33) A Union-level Cybersecurity Reserve should gradually be set up, consisting of services from **trusted** private providers ~~of managed security services~~ to support response and ~~**immediate**~~ **initiate** recovery actions in cases of significant or large-scale cybersecurity incidents. The EU Cybersecurity Reserve should ensure the availability and readiness of services. The services from the EU Cybersecurity Reserve should serve to support national authorities in providing assistance to affected entities operating in **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, Member States should specify the

Commented [A225]: Only trusted private providers are defined in the Act. It gives more flexilibity for fine-tuning exact procurement conditions.

---

1 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December

2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011

support provided to the affected entity at the national level, which should be taken into account when assessing the Member State request. **The CSIRT Network established in Directive EU 2022/2555 can advise the ~~Commission~~ ENISA in 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.

(33a) ~~Having overall responsibility for the implementation of the EU Cybersecurity Reserve, the Commission should~~ ENISA shall **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~~. The contracting authority should consult the Member States regarding the procurement of services to establish the EU Cybersecurity Reserve. ~~Insofar as as the operation and administration of the EU Cybersecurity Reserve has been entrusted, in full or in part, to ENISA, ENISA may be the contracting authority for those services with whose operation and administration it has been entrusted. The procurement procedures to establish the EU Cybersecurity Reserve should be conducted in accordance with Regulation EU 2018/1046. 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 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. 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 in 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 Cyber Reserve should be provided for in the relevant work programmes referred to in**

Commented [A226]: According to NL, this recital is very confusing. NL would like to stress the following **crucial points** that should be reflected in the recitals and legal text:

- **Member States' experts should be involved in the selection of the providers that might be deployed in their own Member State**.
- **Member States should not bear liability following the deployment of the services of the Cyber Reserve.**

Further discussions and amendments regarding this are necessary.

Commented [A227]: According to NL, the 'role of the Member States' should be further specified.

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 NIS Cooperation Group, the Commission should ensure that the views of Member States as regards priorities and 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, ENISA, after consulting the Member States, will ~~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.

Commented [A228]: Member States' experts should be involved in setting the minimum criteria for the selection of providers.

(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,** 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 relevant stakeholders, including representatives from the private sector, Member States, the Commission and other relevant EU institutions, bodies and agencies. As regards the private sector, ENISA is developing channels for exchanging information with specialised providers, including providers of managed security solutions and vendors, in order to contribute to ENISA's mission of achieving a high common level of cybersecurity across the Union. Building on the collaboration with stakeholders, including the private sector, the review report on specific incidents should aim at assessing the causes, impacts and mitigations of an incident, after it has occurred. Particular attention should be

paid to the input and lessons shared by the managed security service providers that fulfil the conditions of highest professional integrity, impartiality and requisite technical expertise as required by this Regulation. The report should be delivered and feed into the work of the EU=-CyCLONe, the CSIRTs network and the Commission. When the incident relates to a third country, it **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 as a whole. Therefore, third countries associated to the DEP may be supported from the EU Cybersecurity Reserve, where this is provided for in the **~~respective association~~ relevant** agreement **or Association Council decision through which ~~to~~ the third country is associated** to DEP. Recognising that support measures of this nature may encompass activities falling within the scope of CSDP Missions or the deployment of military or dual-use technologies, the Commission shall consult with the High Representative and the Council in assessing requests from third countries. In the event that this support is provided to cyber defence authorities or comprises measures falling within the scope of active cyber protection as set out in Directive EU 2022/2555, its deployment should be based on a defensive strategy that excludes offensive measures. As the Union's principal cyber security incident response network, the CyCLONe Network established in Directive EU 2022/2555 shall advise the Commission in reviewing requests for support from the Cyber Reserve. **The CSIRT Network established in Directive EU 2022/2555 ~~can~~ should advise ~~the Commission~~ENISA in reviewing requests for support from the EU Cybersecurity Reserve.** 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~~**.

(37) With the EU Cybersecurity Reserve being available to be used in certain conditions to DEP-associated third countries and the implications such a deployment might have on the EU Common Foreign and Security Policy, it remains important to acknowledge Member States' competences and the role of the High Representative in this field. On the preparation for, the activation and deployment of the EU Cybersecurity Reserve to DEP-associated third countries, the High Representative shall be regularly consulted and coordinated with in order to aim for more coherence, cooperation and consistency in EU foreign and security policy.

(38)

~~(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) […]

HAVE ADOPTED THIS REGULATION:

Chapter I

GENERAL OBJECTIVES, SUBJECT MATTER, AND DEFINITIONS

Article 1

Subject-matter and objectives

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

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

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

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

2. This Regulation pursues the objective to strengthen solidarity at Union level **and enhance**

Member States cyber resilience through **the** following specific objectives:

(a) to strengthen common Union detection and situational awareness of cyber threats and incidents thus allowing to reinforce the competitive position of industry and services sectors in the Union across the digital economy and contribute to the Union's technological sovereignty in the area of cybersecurity;

(b) to reinforce preparedness of entities operating in **sectors of high** critical**ity** and ~~**highly**~~ **other** critical sectors across the Union and strengthen solidarity by developing **enhanced** ~~common~~ response capacities **to handle** ~~against~~ significant or large-scale cybersecurity incidents, including the option to ~~by making~~make Union cybersecurity incident response support available for third countries associated to the Digital Europe Programme

('DEP');

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

3. This Regulation is without prejudice to the Member States' ~~primary~~ sole responsibility for **safeguarding** national security, as stipulated in Article 4 (2) TEU, ~~public security,~~ **and their power to safeguard other essential State functions, including ensuring the territorial integrity of the State and maintaining law and order.** ~~and the prevention, investigation, detection and prosecution of criminal offences.~~

4. Without prejudice to Article 346 TFEU and Article 4(2) TEU, the 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 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.

Commented [A229]: Support for moving this to the legal text and in addition, we would like to add reference to Article 4(2) TEU, specifically with regards to information sharing.

Article 2

Definitions

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

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

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

Commented [A230]: See argumentation above and below on this matter.

(2) **'public body'** means a body governed by public law as defined in Article 2((1), point (4),), of Directive 2014/24/EU of the European Parliament and the Council[1] ~~.~~; For the purpose of this Act, this is a public entity that has the following functionalities:

- it has the capacity to act as a reference point and gateway to other public and private organisations at national level for collecting and analysing ~~information~~ on cyber threats and incidents and contributing to a Cross-border CTI collaboration platform;
- it is capable of detecting, aggregating, and analysing data relevant to cyber threats and incidents by using in particular state of the art technologies;

~~(2)~~(3) **'Hosting Consortium'** means a consortium composed of participating **Member S~~s~~**tates, ~~represented by National SOCs,~~ that have agreed to establish and contribute to the acquisition of tools and infrastructure for, and operation of, a Cross-border SOC **collaboration Platform**;

~~(3)~~(4) '**entity'** means an entity as defined in Article 6, point (38), of Directive (EU) 2022/2555*;*

~~(4)~~(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;

~~(5)~~(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;

~~(6)~~(7) '**significant cybersecurity incident'** means a cybersecurity incident fulfilling criteria set out in Article 23(3) of Directive (EU) 2022/2555;

~~(7)~~(8) '**large-scale cybersecurity incident'** means an incident as defined in Article 6, point (7) 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;

~~(8)~~(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;~~

~~(9)~~(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;~~

~~(10)~~(11) **(8a) 'trusted providers'** means managed security service providers as defined in Article 6, point (40), of Directive (EU) 2022/2555 selected in accordance with Article 16 of this Regulation.

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

Chapter II

THE EUROPEAN ~~CYBER SHIELD~~ CYBERSECURITY ALERT SYSTEM

Article 3

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

1. An interconnected pan-European infrastructure **that consists** of ~~National SOC hubs and~~ **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 detect, analyse and process data on cyber threats and incidents in the Union. ~~It shall consist of all National Security Operations Centres ('National SOCs') and Cross-border Security Operations Centres ('Cross-border SOCs').~~

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

2. The ~~-~~European ~~Cyber Shield~~ **Cybersecurity Alert System** shall, where possible:

(a) pool analysed/aggregated **data** and share **information ~~data~~ as further specified in the written Consortium Agreements as referred to in Article 5 (3),** ~~-~~on cyber threats and incidents from various sources through cross-border ~~SOCs~~ **collaboration platforms**;

(b) **share ~~produce~~** high-quality, actionable information and cyber threat intelligence, through the use of state-of-the art tools **and advanced technologies such as~~, notably~~ ~~A~~a**rtificial ~~I~~**i**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, CSIRTs and the CSIRTs network**;

(d) contribute to **enhanced** ~~faster~~ detection of cyber threats and 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.

Commented [A231]: The Netherlands proposes to use the term "analysed" or "aggregated" throughout articles 3 to 8 of this act when referencing to "information" or "data". The added value of information sharing in this regard would lie in processed data. This would furthermore clearly establish that appropriate measures can be taken with regards to national security, when necessary, since this remains a matter of national competence.

Commented [A232]: This needs to be clarified. Which entities? At national/EU level, public/private entities?

Article 4

Role of National ~~Security Operations Centres~~ ~~Hubs~~

CSIRTs

1. ~~In order~~ **Where a Member State decides** to **voluntarily** participate in the European ~~Cyber Shield~~ **Cybersecurity Alert System**, ~~each Member State~~ **it** shall designate ~~at least one~~ a National ~~SOC Hub~~ CSIRT pursuant to Directive (EU) 2022/2555 or another public body as defined in Article 2(2). ~~The National SOC shall be a public body.~~

~~It shall have the capacity to act as a reference point and gateway to other public and private organisations at national level for collecting and analysing information on cybersecurity threats and incidents and contributing to a Cross-border SOC. It shall be equipped with state-of-the-art technologies capable of detecting, aggregating, and analysing data relevant to cybersecurity threats and incidents.~~

~~2. Following a call for expression of interest, **Member States intending to participate in the European Cyber Shield Cybersecurity Alert System** National SOCs shall be selected by the European Cybersecurity Competence Centre ('ECCC') to **take part** participate in a joint procurement of tools and infrastructures with the ECCC**, in order to set up National SOC hubs or enhance capabilities of an existing one**. The ECCC may award grants to the selected **Member States** National SOCs to fund the operation of those tools and infrastructures. The Union financial contribution shall cover up to 50% of the acquisition costs of the tools and infrastructures, and up to 50% of the operation costs, with the remaining costs to be covered by the Member State. Before launching the procedure for the acquisition of the tools and infrastructures, the ECCC and the **Member State** National SOC shall conclude a hosting and usage agreement regulating the usage of the tools and infrastructures.~~

~~3.~~2. A **Member State** ~~National SOC~~ selected pursuant to paragraph 2 shall commit to apply **for their National** ~~SOC hubs~~CSIRT to participate in a Cross-border ~~SOC~~ **collaboration Platform** within two years from the date on which the tools and infrastructures are acquired, or on which it receives grant funding, whichever occurs sooner. If a **Member State's** National ~~SOC hub~~CSIRT 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

Commented [A233]: We hear the Presidency that it should be up to Member States to designate the exact body on a national level. At the same time, it is of the utmost importance to us that we do not introduce any further complexity in our cyber landscape. The NIS2 has been created to harmonise MS approach to cybersecurity, therefore we should also follow this since the projects are linked to the CSIRT Network. So we see a possible compromise with an explicit reference to national CSIRTs in the operative text (as general principle) but with flexibility to designate another public body, with similar functionalities, if deemed necessary by a Member State.

Cross-border ~~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 ~~SOC hubs work~~CSIRT or another public body, as defined in Article 2(2), ~~working~~** together to

coordinate their cyber-detection and threat monitoring activities shall be eligible to participate in actions to establish a 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 and infrastructures with the ECCC. The ECCC may award to the Hosting Consortium a grant to fund the operation of the tools and infrastructures. The Union financial contribution shall cover up to 75% of the acquisition costs of the tools and infrastructures, and up to 50% of the operation costs, with the remaining costs to be covered by the Hosting Consortium. Before launching the procedure for the acquisition of the tools and infrastructures, the ECCC and the Hosting Consortium shall conclude a hosting and usage agreement regulating the usage of the tools and infrastructures.~~

~~3.~~2. Members of the Hosting Consortium shall conclude a written consortium agreement which sets out their internal arrangements, including specifications regarding information sharing within the cross-border collaboration platform and with the Cybersecurity Alert System, for implementing the hosting and usage ~~A~~**a**greement.

~~4.~~3. A 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 ~~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.**

Commented [A234]: Support

~~5.~~4. **A Member State may join an existing Hosting Consortium with the agreement of all ~~the~~existing 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 and infrastructures already jointly procured with that Hosting Consortium.**

Commented [A235]: Support

Article 6

Cooperation and information sharing within and between cross-border ~~SOCs~~ collaboration Platforms

1. Members of a Hosting Consortium shall **ensure that their National** ~~SOC hubs~~ CSIRTs exchange relevant information**, in accordance with and further specified within the Consortium Agreement,** ~~relevant information~~ among themselves within the 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.** regarding the configuration of cybersecurity tools to detect cyber attacks where such information sharing:

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

   (b) enhances the level of cybersecurity of the Union, in particular through raising awareness in relation to cyber threats, limiting or impeding the ability of such threats to spread, supporting a range of defensive capabilities, vulnerability remediation and disclosure, threat detection, containment and prevention techniques, mitigation strategies, or response and recovery stages or promoting collaborative threat research between public and private entities.

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

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

   (b) a governance framework **clarifying and** incentivising the sharing of information **referred to in paragraph 1** by all participants;

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

3. To encourage exchange of information between Cross-border ~~SOCs~~ **collaboration Platforms**, Cross-border ~~SOCs~~ **collaboration Platforms** shall ensure a high level of interoperability between themselves. To facilitate the interoperability between the Cross-border ~~SOCs~~ **collaboration Platforms**, the Commission may, with the support of ENISA, issue~~,~~ guidance documents ~~by means of implementing acts, after consulting the ECCC, specify the conditions for this interoperability. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2) of this Regulation. Before submitting those draft implementing acts to the committee referred to in Article 21(1),~~

Commented [A236]: NL suggests to simplify the legal text. Cyber threat intelligence (CTI) covers these elements of information already. The type of information shared within a Consortium should be further specified within a Consortium Agreement.

Formatted: Font: (Default) +Headings CS (Times New Roman), Not Bold

~~th~~e Before issuing the guidance documents, the **Commission shall consult the ECCC and existing Cross-border ~~SOC~~ collaboration Platforms.**

4. Cross-border ~~SOCs~~ **collaboration 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. Where the Cross-border ~~SOCs~~ **collaboration Platforms** obtain information relating to a potential or ongoing large-scale cybersecurity incident, they shall **ensure** ~~provide~~ **that** relevant, technical information **is provided** to **the CSIRTs network**~~, EU-CyCLONe, the CSIRTs network, and the Commission, in view of their respective crisis management roles in accordance with Directive (EU) 2022/2555~~ without undue delay. In accordance with the principles for managing large-scale cybersecurity incidents in Directive (EU) 2022/2555 and their standard operating procedures, the CSIRTs network shall notify and share this information with CyCLONe if relevant.

2. ~~The Commission may, by means of implementing acts, determine the procedural arrangements for the information sharing provided for in paragraphs 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2) of this Regulation.~~ Each Cross-border collaboration platform shall ensure that they have procedural arrangements for the information sharing referred to in paragraph 1 of this article.

2. Cross-border collaboration platforms shall, where appropriate, ensure that experiences with state of the art tools, notably Artificial Intelligence and data analytics technology, used within the cross-border collaboration platforms are shared with the CSIRT Network.

Article 8

Security

1. Member States participating in the European ~~Cyber Shield~~ **Cybersecurity Alert System** shall ensure a high level of data security and physical security of the European ~~Cyber Shield~~ **Cybersecurity Alert System** infrastructure, and shall ensure that the infrastructure ~~shall be~~ **is** adequately managed and controlled in such a way as to protect it from threats and to ensure its

Commented [A237]: Crucial for NL to not establish separate information sharing structures. The CSIRTs Network, to which the Commission - through CERT-EU - is a member, would be the designated network to receive this information.

Commented [A238]: Arrangements with regard to information sharing should be up to the Members of the Consortia.

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 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.

Commented [A239]: Support.

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** paragraph~~s~~ 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.**~~

Chapter III

CYBER EMERGENCY MECHANISM

[…]

Article 10

Type of actions

[…]

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

1. As a part of the Mechanism, an Emergency Fund shall be established to rapidly cover immediate costs of Member States necessary for their swift response to significant and large-scale cybersecurity incidents.

Commented [A240]: NL is a strong advocate for establishing a Fund. Happy to work together with the Presidency, Commission and other Member States to further work out this idea.

Article 11

~~Coordinated preparedness testing of entities~~**Preparedness actions**

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

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

2. The NIS Cooperation Group in coordination with EU-CyCLONe ~~in cooperation with the~~ supported by the Commission, ENISA, and the High Representative, shall develop common risk scenarios and methodologies for the **coordinated testing exercises under Article 10 (1) (a) (i). The NIS Cooperation Group, in cooperation with Commission, ENISA and the High Representative, ~~may~~ shall develop common risk scenarios and methodologies for other preparedness actions under Article 10(1)(a)(ii).**

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, responding or providing support for responding to significant or large-scale cybersecurity incidents, and ~~immediate~~ ~~initiate~~ recovery from such incidents.

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

Commented [A241]: In accordance with Art. 10 (1i and ii), this article should have a broader scope with regard to preparedness actions and should not just focus on the testing of entities.

Even more, significant information is missing on how the processes and procedures for preparedness actions will work in practice. Additional texts are needed on the financial procedures (grants ECCC?), roles and responsibilities, the sort of preparedness actions (non-exhaustive) since only pentesting seem to be unnecessary limitative. This needs to be added to this article or should be covered in a new article. Only limited information is already covered in article 19.

Commented [A242]: Support

Commented [A243]: Art. 10(1) point a refers to both testing and other preparedness actions.

Commented [A244]: It is of crucial importance to NL to have a Cybersecurity Reserve that is effective and well-functioning in practice.
We have made a first step towards this end by means of the following initial text proposals. However, at the same time there is still a lot of discussion and work needed to develop a system that works effectively, and due to a lack of time we have not yet been able to convert everything into concrete text proposals. We therefore urge to continue the much needed discussions on this in the Working Party in order be able to make the necessary amendments in the legal text.

all Member States **and in third countries referred to in Article 17 (1).**

3. ~~Users~~ Entities that can apply ('the applicant') ~~of~~ for the services from the EU Cybersecurity Reserve shall include:

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

   (b) ~~Union institutions, bodies and agencies.~~CERT-EU

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

4. Users of the EU Cybersecurity Reserve shall include applicants referred to in paragraph 3 or entities operating in the sectors of high criticality or other critical sectors.

5. ~~Users~~ Applicants referred to in paragraph 3, point (a), shall use the services **granted upon their request** from the EU Cybersecurity Reserve in order to respond or support response to and **initiate** ~~immediate~~ recovery from significant or large-scale incidents affecting entities operating in **sectors of high** critical**ity** or ~~**highly other**~~ critical sectors.

~~4.~~6.

~~5.~~7. The Commission shall have a shared responsibility ~~**have overall responsibility with the**~~ **Member States** for the implementation of the EU Cybersecurity Reserve. **To that end, the** Commission**, in cooperation with the NIS Cooperation Group and ENISA,** shall determine the priorities and evolution of the EU Cybersecurity Reserve, in line with the requirements of the users referred to in paragraph 3, The European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) shall monitor the ~~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 programmes pursuant to the Competence Centre' strategic tasks as outlined in article 5 of EU 2021/887. **These priorities shall be revised every two years.**

~~6. The Commission may~~ENISA **~~shall~~** be responsible for ~~entrust~~ the establishment, operation and administration of the EU Cybersecurity Reserve~~, in full or in part,~~ to ENISA, by means of contribution agreements.

~~7.~~8. ~~In order to support the Commission in establishing the EU Cybersecurity Reserve,~~ ENISA

Commented [A245]: There is a lot of information on how the deployment works on request of Member States, but there is no information included on how processes would work for EUIBAs. Following the logic for Member States it should be CERT-EU requestiong assistance on behalf of an EUIBA, when CERT-EU couldn't handle an incident alone. Throughout the text full allignment is needed with the Act on a High Level of Cybersecurity of EUIBAs and it should be spelled out how the mechanisms would apply and work for EUIBAs.

Commented [A246]: There should be flexibility as is shown with the ENISA pilot. Beneficiaries could be both national CSIRTs as well as NIS2 entities.

Commented [A247]: There should be flexibility as is shown with the ENISA pilot. Beneficiaries could be both national CSIRTs as well as NIS2 entities.

Commented [A248]: Possibly through the ECCC (?).

shall prepare a mapping of the services needed **and their availability**, after consulting **~~Member States~~ the NIS Cooperation Group and, where applicable, the Interinstitutional Cybersecurity Board ~~and the Commission~~** to support the establishment of the EU Cybersecurity Reserve. ENISA shall prepare a similar mapping, after consulting the **the NIS Cooperation Group and the** Commission, to identify the needs of third countries eligible for support from the EU Cybersecurity Reserve pursuant to Article 17. ~~The Commission~~ENISA, ~~where relevant, may shall~~ ~~shall~~ shall take into account the opinions of the NIS Cooperation Group and the High Representative, if such are provided ~~seek the views of consult the High Representative~~.

Commented [A249]: Since EUIBAs can also be users of the services from the EU Cybersecurity Reserve.

~~8.~~9. The Commission may, with the support of ENISA, and after consulting the EU-CyCLONe, by means of ~~implementing acts~~guidance documents, 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). ~~Before submitting those drafting implementing acts to the committee referred to in Article 21(1), the Commission may exchange advice and cooperate with the NIS Cooperation Group.~~

Article 13

Requests for support from the EU Cybersecurity Reserve

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

2. To receive support from the EU Cybersecurity Reserve, the ~~users~~ applicants and their providers referred to in Article 12(3) shall exhaust all other ~~take 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.

Commented [A250]: It is of crucial importance to NL that the Reserve is used as a last resort.

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

Commented [A251]: How will this be arranged for EUIBAs?

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

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

(a) appropriate information on how the provisions of article 9 and 10 of NIS2 Directive have been met as regard~~sing~~ the affected entity and potential impacts of the incident **on affected Member State(s) and users, including the risk of spill over,** and the planned use of the requested support, including an indication of the estimated needs;

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

(c) **where relevant, available** information about other forms of support available to the affected entity~~, including contractual arrangements in place for incident response and initial immediate recovery services, as well as insurance contracts potentially covering such type of incident.~~.

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

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

~~7. The Commission may, by means of implementing acts, specify further the detailed arrangements for allocating the EU Cybersecurity Reserve support services. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2).~~

Commented [A252]: It is unclear what these implementing acts could potentially entail and why these are necessary.

Article 14

Commented [A253]: NL strongly emphasizes that, in order to be able to support the Cyber Reserve proposal, we expect a much stronger role for the Council with regard to the deployment of the Reserve. We are open to looking at a different model for internal and external deployment; this requires further discussions.

Implementation of the support from the EU Cybersecurity Reserve

1. Requests for support from the EU Cybersecurity Reserve, shall be assessed by ENISA ~~the Commission, with the support of ENISA or as defined in contribution agreements under Article 12(6)~~, and a ~~response~~ decision shall be transmitted to the users referred to in Article 12(3) 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 may consult the CSIRTs Network~~-~~ when assessing requests.

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

   (a) the severity of the cybersecurity incident;

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

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

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

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

   (f) the category of ~~user~~ applicants under Article 12(3) of this Regulation, with higher priority given to Member State users and Union institutions, bodies and agencies.

3. The EU Cybersecurity Reserve services shall be provided in accordance with specific agreements between the service provider and the user to which the support under the EU Cybersecurity Reserve is provided. Those agreements shall include liability conditions.

4. ENISA will provide the applicant with multiple options of trusted private providers. The applicant may decide to refuse the offer.

~~3.~~

~~4.~~5. The agreements referred to in paragraph 3 may be based on templates prepared by ENISA, after consulting Member States.

Commented [A254]: Support

Commented [A255]: Support

Commented [A256]: More information in the text or in a recital is needed on how the process works when a request has been accepted, would applicants be able to choose from the total list, a subset, or will ENISA select the provider for a MS? If so, can MS decline and would they receive a new offer?

5.6. ~~The Commission and~~ Applicants ~~ENISA~~ shall bear no contractual liability for damages caused to third parties by the services provided in the framework of the implementation of the EU Cybersecurity Reserve.

6.7. Within **three** ~~one~~ month**s** from the end of the support action, the ~~users~~ applicant shall provide **the** Commission**,** ~~and~~ ENISA**, the CSIRTs network and, where appropriate, EU-CyCLONe** with a summary report about the service provided, results achieved and the lessons learned. When the user is from a third country as set out in Article 17, such report shall be shared with the High Representative.

8. ~~The Commission~~ENISA shall report to Commission and the NIS Cooperation Group**, on a regular basis and at least** ~~once~~ **twice a**~~per~~ **year,** about the use and the results of the support~~, on a regular basis~~.

Commented [A257]: Liability questions still need further discussion and clarification throughout the text. Information is missing to properly assess whether this clause is justifiable. This also depends on MS involvement with establishing the list of trusted providers and flexibility to choose a suitable provider for the task at hand.
Similarly, when deploying the reserve in a third country, who will be potentially liable?

[…]

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:

Commented [A258]: This list of 'trusted provider' might also be of great interest to our adversaries. Would there be possibilities for a non-public list to be accessed by users only?

[…]

Article 17

Support to DEP-associated third countries

[…]

1. The Commission shall **inform and consult the NIS Cooperation Group** ~~**Council**~~ **and cooperate**~~coordinate~~ with the High Representative about the requests received and the implementation of the support granted to third countries from the EU Cybersecurity Reserve. **The Commission shall take into account the opinions of the NIS Cooperation Group and the High Representative, if such are provided.**

[…]

---

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

[…]

Chapter V

FINAL PROVISIONS

Article 19

Amendments to Regulation (EU) 2021/694

Commented [A259]: The amendments to regulation (2021/694) should reflect the position of the Council in the rest of the legal text (this still needs to be adapted in some places).

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

(1) Article 6 is amended as follows:

(a) paragraph 1 is amended as follows:

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

'(aa) support the development of an EU ~~Cyber Shield~~ **Cybersecurity Alert System**, including the development, deployment and operation of National and Cross-border SOC**s 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';

(b) Paragraph 2 is replaced by the following:

'2. The actions under Specific Objective 3 shall be implemented primarily through the European Cybersecurity Industrial, technology and research Competence Centre and the Network of National Coordination Centres, in accordance with Regulation (EU) 2021/887 of the European Parliament and of the Council[1] with the exception of actions implementing the EU Cybersecurity Reserve, which shall be implemented by the ~~Commission and~~ ENISA.**';**

(2) Article 9 is amended as follows:

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

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

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

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

(b) the following paragraph 8 is added:

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

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

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

---

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

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.

Commented [A260]: Should reflect the wish for Council involvement.

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~~ two 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.

Commented [A261]: Act should be evaluated before next MFF

[…]

AUSTRIA

[…]

Whereas:

[…]

(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[70], it is necessary to increase the resilience of citizens, businesses and entities operating critical infrastructures against the growing cybersecurity threats, which can have devastating societal and economic impacts. Therefore, investment in infrastructures and services that will support faster detection and response to cybersecurity threats and incidents is needed, and Member States need assistance in better preparing for, as well as responding to significant and large-scale cybersecurity incidents. **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.

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

[…]

(7) It is necessary to strengthen the detection and situational awareness of cyber threats and incidents throughout the Union and to strengthen solidarity by enhancing Member States' and the Union's preparedness and capabilities to respond to significant and large-scale cybersecurity incidents. Therefore a pan-European infrastructure of SOCs (European Cyber**security** ~~Shield~~ **Alert System**) should be deployed 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**, with due respect for Member State competences and without duplication of the activities conducted by the CSIRT network, EU-CyCLONe and the NIS Cooperation Group**. These actions shall be without prejudice to Articles 107 and 108 of the Treaty on the Functioning of the European Union ('TFEU').

(8) To achieve these objectives, it is also necessary to amend Regulation (EU) 2021/694 of the European Parliament and of the Council[71] 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 DEP, which aims at guaranteeing the resilience, integrity and trustworthiness of the Digital Single Market, at strengthening capacities to monitor cyber-attacks and threats and to respond to them, and at reinforcing cross-border cooperation on cybersecurity. This will be complemented by the specific conditions under which financial support may be granted for those actions should be established and the governance and coordination mechanisms necessary in order to achieve the intended objectives should be defined. Other amendments to Regulation (EU) 2021/694 should include descriptions of proposed actions under the new operational objectives, as well as measurable indicators to monitor the implementation of these new operational objectives.

[…]

(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

---

[71] 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).

infrastructures on the territory of the Union, including their geographical distribution, interconnection and potential effects in case of cyber-attacks affecting those infrastructures. A large-scale Union infrastructure of SOCs should be deployed ('the European Cyber**security** ~~Shield~~ **Alert System**'), comprising of several interoperating cross-border collaboration platforms, each grouping together several National SOC hubs. That infrastructure should serve national and Union cybersecurity interests and needs, leveraging state of the art technology for advanced collection of anonymized and relevant data ~~collection~~ and analytics tools, enhancing cyber detection and management capabilities and providing real-time situational awareness. That infrastructure should serve to increase detection of cybersecurity threats and incidents and thus complement and support Union entities and networks responsible for crisis management in the Union, notably the EU Cyber Crises Liaison Organisation Network ('EU-CyCLONe'), as defined in Directive (EU) 2022/2555 of the European Parliament and of the Council[72].

Commented [A262]: It is highly important for AT that data shared is anonymized. Furthermore, we want to emphasize that only data that brings significant value for detection and monitoring threats ("relevant") should be shared.

(13) **Participation in the European ~~Cyber Shield~~ Cybersecurity Alert System should be voluntary for Member States.** Each Member State **that decides to join the European ~~Cyber Shield~~ Cybersecurity Alert System** should designate a **National SOC hub.** ~~public body at national level tasked with coordinating cyber threat detection activities in that Member State.~~ These National SOC~~s~~ **hubs** should **have** ~~act~~ as **functionalities the capacity to act as** a reference point and gateway at national level for participation in the European ~~Cyber Shield~~ **Cybersecurity Alert System** and should **be capable of detecting, aggregating and analysing data relevant to cyber threats and incidents, by using in particular state-of-the-art technologies** ~~and that would be shared appropriately with the CSIRT network in order to support the network 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.** When participating in the Cybersecurity Alert System **Member States** ~~should be able to~~**may** ~~decide to~~ **designate an existing entity such as a CSIRT,** ~~,~~ **its SPOC referred to in Art 8.3 of the Regulation (EU) 2022/2555 or other existing national platforms 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.**

Commented [A263]: We would appreciate this addition.

[72] 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).

(14) As part of the European Cyber**security Alert System** ~~Shield~~, a number of Cross-border Cybersecurity Operations Centres ('Cross-border SOCs') should be established. These should bring together National SOC hubs 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 SOC collaboration plattforms 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 **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.~~

Commented [A264]: Alternatively, we would like to suggest the following modification:

They should provide new additional capacity, building upon and complementing existing *National* SOC *Hubs tasks, irrespective by whom they may be performed.*

(14a) A Member State selected by the European Cybersecurity Competence Centre (ECCC) following a call for expression of interest to set up a National SOC Hub or enhance the capabilities of an existing one, should jointly purchase relevant tools and infrastructures with the ECCC. Such a Member State should be eligible to receive a grant to operate the tools and infrastructures. 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 collaboration SOC Platform or enhance the capabilities of an existing one, should jointly purchase relevant tools and infrastructures with the ECCC. Such a Hosting Consortium should be eligible to receive a grant to operate the tools and infrastructures. 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 procurement procedure to purchase the relevant tools and infrastructures should be carried out jointly by the ECCC and relevant contracting authorities from the Member States selected following these calls for expressions of interest. Private entities should therefore not be eligible to participate in the calls for expression of interest to jointly purchase tools and infrastructures with the ECCC, or to receive grants to operate those tools and infrastructures. However, the Member States should have the possibility to involve private entities in the setting up, enhancement and operation of their National SOC Hubs and Cross-border SOCs Platforms in other ways which they deem appropriate, in compliance with national and Union law.

(15) At national level, the monitoring, detection and analysis of cyber threats is typically ensured by SOCs of public and private entities, in combination with CSIRTs. In addition, CSIRTs exchange information in the context of the CSIRT network, in accordance with Directive (EU) 2022/2555. The Cross-border SOCs should constitute a new capability that is complementary to the CSIRTs network **and will cooperate closely with it,** by pooling **data** and sharing **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 SOCs should act as a central point allowing for a broad pooling of relevant data and cyber threat intelligence, enable the spreading of threat information among a large and diverse set of actors (e.g., Computer Emergency Response Teams ('CERTs'), CSIRTs, Information Sharing and Analysis Centers ('ISACs'), operators of critical infrastructures). The information exchanged among participants in a Cross-border SOC could include anonymized data from networks and sensors, which adds significant value to threat detection and monitoring, threat intelligence feeds, indicators of compromise, and contextualised information about incidents, threats and vulnerabilities. In addition, Cross-border SOCs should also enter into cooperation agreements with other Cross-border SOCs.

[…]

(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**~~ cause**s** ~~**and impacts** of cybersecurity~~ **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 should be able to issue guidance in this respect.** This should make it possible to improve collective detection capacities and timely warnings to authorities and relevant entities, notably by using the latest ~~artificial intelligence and~~ data analytics technologies.

(20) By collecting, **correlating,** sharing and exchanging **data and information**, the European ~~Cyber Shield~~ **Cybersecurity Alert System** should enhance the Union's technological sovereignty. The pooling of anonymized and relevant high-quality curated data should also contribute to the development of advanced artificial intelligence and data analytics technologies. It should be facilitated through the connection of the European ~~Cyber Shield~~ **Cybersecurity Alert System** with the pan-European High Performance Computing infrastructure established by Council Regulation (EU) 2021/1173[73].

(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 'High Representative'), should gradually develop dedicated protocols and standards to allow for cooperation with the cyber defence community, including vetting and security conditions. The development of the European Cyber**security 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.

(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.

~~**(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**~~

[73] 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).

~~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 as a crisis support instrument is being introduced,** to improve the Union's resilience to significant and large-scale cybersecurity incidents and complement Member States' actions through emergency financial support for preparedness, response and **initial** ~~**immediate**~~ recovery of ~~essential~~ services provided by an essential or important entity. That instrument should enable the rapid deployment of assistance in defined circumstances and under clear conditions and allow for a careful monitoring and evaluation of how resources have been used. Whilst the primary responsibility for preventing, preparing for and responding to cybersecurity incidents and crises lies with the Member States, the Cyber Emergency Mechanism promotes solidarity between Member States in accordance with Article 3(3) of the Treaty on European Union ('TEU').

(25) The Cyber Emergency Mechanism should provide support to Member States complementing their own measures and resources, and other existing support options in case of response to and ~~**immediate**~~ **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[74] ~~**and Hybrid Rapid Response Teams**~~. It should address the need to ensure that specialised means are available to support preparedness and response to cybersecurity incidents across the Union and in third countries.

(26) This ~~**instrument**~~**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**~~[75], **the EU Integrated Political Crisis Response Arrangements under Council Implementing Decision (EU) 2018/1993**~~**IPCR**~~[76] **(IPCR Arrangements),**

---

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

75 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).

76 **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.**

Commission Recommendation 2017/1584[77] 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**~~. Support provided under the Cyber Emergency Mechanism can~~ and 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.

[…]

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

Commented [A265]: In order to better align with NIS2.

(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

~~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.~~

[77] **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).**

assessing cybersecurity of entities operating in ~~highly critical~~ sectors **of high criticality** identified pursuant to Directive (EU) 2022/2555 in a coordinated manner. For this purpose, the Commission, after consulting the NIS Cooperation Group established by Directive (EU) 2022/2555and ENISA, shall ~~with the support of ENISA and in cooperation with the NIS Cooperation Group established by Directive (EU) 2022/2555, should~~ regularly identify relevant sectors or subsectors, which should be eligible to receive financial support for coordinated testing at Union level. The sectors or subsectors should be selected from Annex I to Directive (EU) 2022/2555 ('Sectors of High Criticality'). The coordinated testing exercises should be based on common risk scenarios and methodologies. The selection of sectors and development of risk scenarios should take into account relevant Union-wide risk assessments and risk scenarios, including the need to avoid duplication, such as the risk evaluation and risk scenarios called for in the Council conclusions on the development of the European Union's cyber posture ~~to be~~ conducted by the Commission, the High Representative and the NIS Cooperation Group, in coordination with relevant civilian and military bodies and agencies and established networks, including the EU CyCLONe, as well as the risk assessment of communications networks and infrastructures requested by the Joint Ministerial Call of Nevers and conducted by the NIS Cooperation Group, with the support of the Commission and ENISA, and in cooperation with the Body of European Regulators for Electronic Communications (BEREC), the coordinated risk assessments to be conducted under Article 22 of Directive (EU) 2022/2555 and digital operational resilience testing as provided for in Regulation (EU) 2022/2554 of the European Parliament and of the Council[78]. 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.

Commented [A266]: To align the wording with Art 11.1.

(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 cristical sectors. Those actions could include various types of national preparedness activities.

Commented [A267]: To align the wording with Art 10.

(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

[78] 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

appropriate, it should complement the UCPM to ensure a comprehensive approach to respond to the impacts of cyber incidents on citizens.

[…]

(33) 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 or large-scale cybersecurity incidents. The EU Cybersecurity Reserve should ensure the availability and readiness of services. The services from the EU Cybersecurity Reserve should serve to support national authorities in providing assistance to affected entities operating in **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, Member States should specify the support provided to the affected entity at the national level, which should be taken into account when assessing the Member State request. ~~**The CSIRT Network established in Directive EU 2022/2555 can advise the Commission in 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.

Commented [A268]: This is not represented in Art 14.1.

(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, ENISA may be the contracting authority for those services with whose operation and administration it has been entrusted. The procurement procedures to establish the EU Cybersecurity Reserve should be conducted in accordance with Regulation EU 2018/1046. 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 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. 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~~ ought to be based on templates prepared by ENISA, after consulting Member States.

(33b) Due regard should be given to the role of the Member States in 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 Cyber 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 NIS Cooperation Group, the Commission should ensure that the views of Member States as regards priorities and evolution of the EU Cybersecurity Reserve are taken into account.

(33c) To promote cooperation beyond the borders of the European Union, third countries whose association agreements provide for it may request support from the European Cybersecurity Reserve.

Commented [A269]: Recital on third countries missing.

(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. The call for tenders should wherever legally prossible make use of the limitation possibility set out in Art 12.5 of Regulation (EU) 2021/694.

(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,** 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 relevant stakeholders, including representatives from the private sector, Member States, the Commission and other relevant EU institutions, bodies and agencies. As regards the private sector, ENISA is developing channels for exchanging information with specialised providers, including providers of managed security solutions and vendors, in order to contribute to ENISA's mission of achieving a high common level of cybersecurity across the Union. Building on the collaboration with stakeholders, including the private sector, the review report on specific incidents should aim at assessing the causes, impacts and mitigations of an incident, after it has occurred. Particular attention should be paid to the input and lessons shared by the managed security service providers that fulfil the conditions of highest professional integrity, impartiality and requisite technical expertise as required by this Regulation. The report should be delivered and feed into the work of the EU~~=~~-CyCLONe, the CSIRTs network and the Commission. When the incident relates to a third country, it **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 as a whole. Therefore, third countries associated to the DEP may be supported from the EU Cybersecurity Reserve, where this is provided for in the ~~respective association~~ **relevant** agreement **or Association Council decision through which ~~to~~ the third country is associated** to DEP. **The CSIRT Network established in Directive EU 2022/2555 can advise the Commission in reviewing requests for support from the EU Cybersecurity Reserve.** 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~~.

(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.

[…]

HAVE ADOPTED THIS REGULATION:

Chapter I

GENERAL OBJECTIVES, SUBJECT MATTER, AND DEFINITIONS

Article 1

Subject-matter and objectives

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

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

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

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

2. This Regulation pursues the objective to strengthen solidarity at Union level **and enhance Member States cyber resilience** through **the** following specific objectives:

   […]

   (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 capacities **to handle** ~~against~~ significant or large-scale cybersecurity incidents, including by making Union cybersecurity incident response

support available for third countries associated to the Digital Europe Programme ('DEP');

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

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

4. Without prejudice to Article 346 TFEU, the 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 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.

Article 2

Definitions

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

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

(a) it has the capacity to act as a reference point and gateway to other public and private organisations at national level for collecting and analysing ~~information~~ on cyber threats and incidents and contributing to a Cross-border SOC 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 Security Operations Centre collaboration Platform' ("Cross-border SOC collaboration Platform**") means a multi-country platform, **established by a written consortium agreeement** that brings together in a coordinated network structure **N~~n~~**ational

Commented [A270]: Is it possible to receive further information of what is meant by that?
The explanation should possibly be included in the recitals as well.

Commented [A271]: This needs so be replaced by another word – otherwise this does not make much sense.

SOC~~s~~ **Hubs** from at least three Member States ~~who form a Hosting Consortium~~, and that is designed to **monitor, detect and analyse** ~~prevent~~ cyber threats ~~and~~ **to prevent** incidents and to support the production of **cyber threat** ~~high-quality~~ intelligence, notably through the exchange of anonymized ~~**information** **data** from various sources, public and private~~, which adds a significant value to monitoring and detecting cyber threats, 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[79];~~

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

(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;

(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;

~~(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;~~

[79] 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).

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

~~(11)~~ **(8a) 'trusted providers'** means managed security service providers as defined in Article 6, point (40), of Directive (EU) 2022/2555 selected in accordance with Article 16 of this Regulation.

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

Chapter II

THE EUROPEAN ~~CYBER SHIELD~~ CYBERSECURITY ALERT SYSTEM

Article 3

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

1. An interconnected pan-European infrastructure **that consists** of **National SOC hubs and Cross-border SOC collaboration platforms joining on a voluntary basis** ~~Security Operations Centres ('European Cyber Shield~~ **the European Cybersecurity Alert System**~~')~~ shall be established to **support the** develop**ment of** advanced capabilities for the Union to detect, analyse and process data on cyber threats and incidents in the Union. ~~It shall consist of all National Security Operations Centres ('National SOCs') and Cross-border Security Operations Centres ('Cross-border SOCs').~~

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

2. The European ~~Cyber Shield~~ **Cybersecurity Alert System** shall:

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

   (b) **share** ~~**produce**~~ high-quality, actionable information and cyber threat intelligence, through the use of state-of-the art tools **and advanced technologies such as**~~, notably A~~**a**rtificial ~~I~~**i**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, CSIRTs and the CSIRTs network**;

(d) contribute to **enhanced** ~~faster~~ detection of cyber threats and 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 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 designate at least one National SOC **Hub**. ~~The National SOC shall be a public body.~~

   ~~It shall have the capacity to act as a reference point and gateway to other public and private organisations at national level for collecting and analysing information on cybersecurity threats and incidents and contributing to a Cross-border SOC. It shall be equipped with state-of-the-art technologies capable of detecting, aggregating, and analysing data relevant to cybersecurity threats and incidents.~~

2. Following a call for expression of interest, **Member States intending to participate in the European ~~Cyber Shield~~ Cybersecurity Alert System** ~~National SOCs~~ shall be selected by the European Cybersecurity Competence Centre ('ECCC') to **take part** ~~participate~~ in a joint procurement of tools and infrastructures with the ECCC**, in order to set up National SOC hubs or enhance capabilities of an existing one**. The ECCC may award grants to the selected **Member States** ~~National SOCs~~ to fund the operation of those tools and infrastructures. The Union financial contribution shall cover up to 50% of the acquisition

costs of the tools and infrastructures, and up to 50% of the operation costs, with the remaining costs to be covered by the Member State. Before launching the procedure for the acquisition of the tools and infrastructures, the ECCC and the **Member State** ~~National SOC~~ shall conclude a hosting and usage agreement regulating the usage of the tools and infrastructures.

3. A **Member State** ~~National SOC~~ selected pursuant to paragraph 2 shall commit to apply **for their National SOC hubs** to participate in a Cross-border SOC **collaboration Platform** within two years from the date on which the tools and infrastructures are acquired, or on which it receives grant funding, whichever occurs sooner. If a **Member State's** National SOC **hub** is not a participant in a Cross-border SOC **collaboration Platform** by that time, **the Member State** ~~it~~ shall not be eligible for additional Union support under this **Chapter** until it has joined a Cross-border SOC collaboration Platform ~~Regulation~~.

Article 5

Cross-border Security Operations Centre~~s~~ collaboration Platforms

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

[…]

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.

4. A 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 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 and infrastructures already jointly procured with that Hosting Consortium.

Article 6

Cooperation and information sharing within and between cross-border SOC~~s~~ collaboration Platforms

1. Members of a Hosting Consortium shall **ensure that their National SOC hubs** exchange**, in accordance with the Consortium Agreement,** relevant information among themselves within the Cross-border SOC **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:

   […]

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

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

   (b) a governance framework **clarifying and** incentivising the sharing of information **referred to in paragraph 1** by all participants;

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

3. To encourage exchange of information between Cross-border SOC~~s~~ **collaboration Platforms**, Cross-border SOC~~s~~ **collaboration Platforms** shall ensure a high level of interoperability between themselves. To facilitate the interoperability between the Cross-border SOC~~s~~ **collaboration Platforms**, Cross-border SOC~~s~~ collaboration Platforms shall conclude cooperation agreements with one another, specifying establising interoperablity as well as information sharing principles among the cross-border platforms. ~~t~~The Commission may issue guidance to support establishing interoperablity. ~~, by means of implementing acts, after consulting the ECCC, specify the conditions for this interoperability. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2).~~

~~4. The Commission may, by means of implementing acts, after consulting the ECCC, establish the conditions for interoperability between Cross-border SOC collaboration Platforms.~~

Commented [A272]: Moved to Art 6.3.

Article 7

Cooperation and information sharing with Union-level entities and networks

1) Irrespective of a cybersecurity incident Cross border SOC collaboration Platforms and the CSIRTs Network shall cooperate closely. For that purpose, they shall agree on procedural arrangements and cooperate and share information on cybersecurity threats from public and private entities on the basis thereof.

1a. Where the Cross-border SOC~~s~~ **collaboration Platforms** obtain information relating to a potential or ongoing large-scale cybersecurity incident, they shall **ensure** ~~provide~~ **that** relevant information **is provided** to **the CSIRTs network,** EU-=CyCLONe, ~~the CSIRTs network,~~ and the Commission, in view of their respective crisis management roles in accordance with Directive (EU) 2022/2555 through existing national channels without undue delay.

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

Commented [A273]: We support the position of DE & others to delete this implementing act. As there are many other ways to share information, we do not see the necessity of this implementing act.

Article 8

Security

1. Member States participating in the European ~~Cyber Shield~~ **Cybersecurity Alert System** shall ensure a high level of data security and physical security of the European ~~Cyber Shield~~ **Cybersecurity Alert System** infrastructure, and shall ensure that the infrastructure ~~shall be~~ **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 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.

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 paragraph**s** 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.

Chapter III

CYBER EMERGENCY MECHANISM

Article 9

Establishment of the Cyber Emergency Mechanism

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

[…]

Article 10

Type of actions

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

(a) preparedness actions**:**~~, including~~

(xi) the coordinated preparedness testing of entities operating in **sectors of high criticality** ~~highly critical sectors~~ across the Union;

(xii) other preparedness actions for entities operating in sectors of high criticality ~~**critical**~~ **and other** ~~**highly**~~ **critical sectors, including those involving exercises and trainings and ;**

(b) ~~response~~ actions~~,~~ supporting response to and **initiating** ~~immediate~~ recovery from significant and large-scale cybersecurity incidents, to be provided by trusted providers participating in the EU Cybersecurity Reserve established under Article 12;

(c) mutual assistance actions regarding significant or large-scale cybersecurity incidents 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.

Commented [A274]: To ensure consistency with recital 32.

Commented [A275]: We understand from previous explanations of the EC that there should be grant without a call to provide for funding. Could you please elaborate on how this would work in practice?

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

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

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

2. The NIS Cooperation Group in cooperation with the Commission, ENISA, and the High Representative, shall develop common risk scenarios and methodologies for the **coordinated testing exercises under Article 10 (1) (a) (i). The NIS Cooperation Group, in cooperation with Commission, ENISA and the High Representative, may develop common risk scenarios and methodologies for other preparedness actions under Article 10(1)(a)(ii).**

Article 12

Establishment of the EU Cybersecurity Reserve

Commented [A276]: Re the overall competences on the Cybersecurity Reserve, we support the position put forward by many for an overall stronger role of the member states as well as clear competences, while not creating new structures and bodies.

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

2. The EU Cybersecurity Reserve shall consist of incident response services from trusted providers selected in accordance with the criteria laid down in Article 16. The Reserve shall

include pre-committed services. The ~~services~~ **Reserve shall** be deployable **upon request** in all Member States **and in third countries referred to in Article 17 (1).**

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

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

   (b) Union institutions, bodies and agencies.

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

4. Users referred to in paragraph 3, point (a), shall use the services **granted upon their request** from the EU Cybersecurity Reserve in order to respond or support response to and **initiate** ~~immediate~~ recovery from significant or large-scale incidents affecting entities operating in **sectors of high** critical**ity** or ~~**highly**~~ **other** critical sectors.

5. The Commission shall responsibility **have overall responsibility** for the implementation of the EU Cybersecurity Reserve. **To that end, the** Commission**, in cooperation with the NIS Cooperation Group and ENISA,** shall determine the priorities and evolution of the EU Cybersecurity Reserve, in line with the requirements of the users referred to in paragraph 3, and shall supervise its implementation, and ensure complementarity, consistency, synergies and links with other support actions under this Regulation as well as other Union actions and programmes. **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 a mapping of the services needed **and their availability**, after consulting ~~**Member States**~~ **the NIS Cooperation Group** and the Commission. ENISA shall prepare a similar mapping, after consulting the **the NIS Cooperation Group and the** Commission, to identify the needs of third countries eligible for support from the EU Cybersecurity Reserve pursuant to Article 17. The Commission, where relevant, **may** ~~shall~~ **seek the views of** ~~**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). **Before submitting those drafting implementing acts to the committee referred to in Article**

21(1), the Commission ~~may~~ shall consult, exchange advice and cooperate with the NIS Cooperation Group.

Article 13

Requests for support from the EU Cybersecurity Reserve

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

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

[…]

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

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

   (a) appropriate information regarding the affected entity and potential impacts of the incident **on affected Member State(s) and users, including the risk of spill over,** and the planned use of the requested support, including an indication of the estimated needs;

   (b) 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.

[…]

Article 14

Implementation of the support from the EU Cybersecurity Reserve

1. Requests for support from the EU Cybersecurity Reserve, shall be assessed by the Commission, with the support of ENISA or as defined in contribution agreements under Article 12(6), and a response shall be transmitted to the users referred to in Article 12(3) without delay **and in any event no later than 72 hours from the submission of the request to ensure effectiveness of the support action**.

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

[…]

(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 and Union institutions, bodies and agencies**~~**users in Art 12(3) point (a) and (b).**

Commented [A277]: Modification just for clarification.

[…]

6. Within **three** ~~one~~ month**s** from the end of the support action, the users shall provide **the** ~~Commission, and~~ ENISA**, the CSIRTs network and**~~, where appropiate,~~ **EU-CyCLONe** with a summary report about the service provided, results achieved and the lessons learned. When the user is from a third country as set out in Article 17, such report shall be shared with the High Representative.

7. The Commission shall report to the NIS Cooperation Group**, on a regular basis and at least once per year,** about the use and the results of the support~~, on a regular basis~~.

~~*Article 15*~~

~~**Coordination with crisis management mechanisms**~~

~~1. In cases where significant or large-scale cybersecurity incidents originate from or result in disasters as defined in Decision 1313/2013/EU[80], the support under this Regulation for responding to such incidents shall complementactions under and without prejudice to Decision 1313/2013/EU.~~

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

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

~~3. In consultation with the High Representative, support under the Cyber Emergency Mechanism may complement assistance provided in the context of the Common Foreign and Security Policy and Common Security and Defence Policy, including through the Cyber Rapid Response Teams. It may also complement or contribute to assistance provided by one Member State to another Member State in the context of Article 42(7) of the Treaty on the European Union.~~

~~4. Support under the Cyber Emergency Mechanism may form part of the joint response between the Union and Member States in situations referred to in Article 222 of the Treaty on the Functioning of the European Union.~~

Article 16

Trusted providers

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

   (a) ensure **that the services included in** the EU Cybersecurity Reserve **are such that the Reserve** ~~includes services that~~ may be deployed in all Member States, taking into account in particular national requirements for the provision of such services, including certification or accreditation;

[…]

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

   […]

   (d) the provider shall have appropriate security clearance, at least for personnel intended for service deployment~~;~~ **, where required by a Member State;**

   […]

(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.

Article 17

Support to DEP-associated third countries

1. **A DEP- associated t**~~**T**~~hird country**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 shall be 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.

[…]

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**, **p**~~**P**~~rior to receiving any support from the EU Cybersecurity Reserve, third countries shall provide to the Commission ~~**and the High Representative**~~ information about their cyber resilience and risk management capabilities, including at least information on national measures taken to prepare for significant or large-scale cybersecurity incidents, as well as information on responsible national entities, including CSIRTs or equivalent entities, their capabilities and the resources allocated to them. **The Commission shall share this information with the High Representative, for the purpose of facilitating the cooperation referred to in paragraph 6**. Where provisions of Articles 13 and 14 of this Regulation refer to Member States, they shall apply to third countries as set out in paragraph 1.

6. The Commission shall **inform the NIS Cooperation Group ~~Council~~ and cooperate~~coordinate~~** with the High Representative about the requests received and the implementation of the support granted to third countries from the EU Cybersecurity Reserve. **The Commission shall take into account the opinions of the NIS Cooperation Group and the High Representative, if such are provided.**

Article 17a) ~~15~~

Coordination with Union crisis management mechanisms

1. **~~In cases w~~Where a significant cybersecurity incident or a large-scale cybersecurity incident~~s~~ originate~~s~~ from or result~~s~~ in a disaster~~s~~ as defined in Article 4, point (1), of Decision No 1313/2013/EU[81], 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~~, 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.**

~~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.~~

---

81 ~~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).~~

Chapter IV

CYBERSECURITY INCIDENT REVIEW MECHANISM

Article 18

Cybersecurity Incident Review Mechanism

1. ~~**After consulting Member States concerned, and A**~~a**t** the request of the Commission, the EU-CyCLONe or the CSIRTs network, **and with the agreement of the Member States concerned,** ENISA shall review and assess threats, vulnerabilities and mitigation actions with respect to a specific significant or large-scale cybersecurity incident. Following the completion of a review and assessment of an incident, ENISA shall deliver an incident review report to the CSIRTs network, the EU-CyCLONe and the Commission to support them in carrying out their tasks, in particular in view of those set out in Articles 15 and 16 of Directive (EU) 2022/2555. ~~**Where relevant,**~~ **When an incident has an impact on a third country**, the Commission shall share the report with the High Representative.

2. To prepare the incident review report referred to in paragraph 1, ENISA shall collaborate all relevant stakeholders, including representatives of Member States, the Commission, other relevant EU institutions, bodies and agencies, managed security services providers and users of cybersecurity services. Where appropriate, **and** ~~**in close cooperation**~~ **with the agreement 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, 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) 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 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 and Cross-border SOC~~s~~ **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';

[…]

(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.

[…]

POLAND

General remarks

- It is necessary to unify the naming in the recitals of the document and in the text of the CSoA proposal itself. This is true both in relation to the original compromise text and to sent amendment proposals. We did not fully reflect our proposals in the recitals

Regarding SOCs:

- The point of introducing a duplicative separate structure to perform cybersecurity tasks in the EU is not acceptable. To properly fulfill tasks and effectively achieve the objectives of the CSoA proposal, it is necessary to clearly differentiate between the tasks of the entities and mechanisms established within the CSoA and those set out in NIS 2. Only this will ensure an efficient, joint, non-duplicative and mutually supportive response to incidents and thus strengthen the common level of cybersecurity in the EU. CSIRTs should have a crucial role it is of utmost importance to ensure non duplication of structures.
- We propose to replace the National Security Operations Centre Hub' ("National SOC hub") with National CSIRT as it is both superfluous and the role described in the CSoA for National SOC hub is already performed by the National CSIRTs. Therefore the word SOC should be deleted
- There should not be any implementing acts in art. 6 and 7
- in art. 7, there should be an automatic notification to the CSIRT network, and depending on their standard operating procedures, CSIRTs could proceed to CyCLONe.
- Ensuring the confidentiality of information is essential
- We can support FR proposal to change name to Cyber Support System
- There should be a framework for cooperation with private companies

Regarding the cyber reserve, we would like to raise the following strong points:

- MS involvement in deployment of the Reserve internally and external is crucial
- ENISA should be the only entity responsible for the implementation of the Reserve – clear tasking has to be done in the act
- The information in the request for support provided by MS should be shared only with ENISA, the EC should not receive it
- There should be a possibility to use reserve also for preparedness with money that is not used for ex post actions – ensure flexibility
- It is still not clear at all how the Reserve will work in practice – as it will not work like the ENISA support action
- The issue of liability is not clear – MS/CSIRT should not be liable, who will be liable?
- EUIBAS have their own budget, they should not use the DEP resource, so they should be deleted as users wholly, as a compromise we can accept puttind cert EU instead
- Why there is a need for precomittment needs to be further explained. We still have concerns
- PL agrees with the overall DE suggestion and proposal to simplify and streamline the process of receiving support from the EU Cybersecurity Reserve, while at the same time emphasize need for further discussion on implications contacting directly with the providers as e.g.:
  - the risk of overloading a limited group of suppliers with work, which would result in a prolonged incident response, and

- no tools or abilities for providers to apply the assessment criteria set out in the article 14(2).

[…]

(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.

Commented [A278]: Is this to be defined in line with the NIS2 ? should be clarified

[…]

(7) It is necessary to strengthen the detection and situational awareness of cyber threats and incidents throughout the Union and to strengthen solidarity by enhancing Member States' and the Union's preparedness and capabilities to respond to significant and large-scale cybersecurity incidents. Therefore a pan-European infrastructure of SOCs (European Cyber**security** ~~Shield~~ **Alert System**) should be deployed 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**, with due respect for Member State competences and without duplication of the activities conducted by the CSIRT network, EU-CyCLONe and the**

Commented [A279]: The name "Cybersecurity Alert System" does not reflect what the articles of the act actually define. Support for FR proposal to change to Cyber Support System

NIS Cooperation Group. These actions shall be without prejudice to Articles 107 and 108 of the Treaty on the Functioning of the European Union ('TFEU').

Commented [A280]: the competences and their division should be clearly defined in the proposal, not only in recitals.

[…]

(12) To more effectively prevent, assess and respond to cyber threats and incidents, it is necessary to develop more comprehensive knowledge about the threats to critical assets and infrastructures on the territory of the Union, including their geographical distribution, interconnection and potential effects in case of cyber-attacks affecting those infrastructures. A large-scale Union infrastructure of SOCs should be deployed ('the European Cyber**security** ~~Shield~~ **Alert System**'), comprising of several interoperating cross-border platforms, each grouping together several National ~~SOCs~~ hubs. That infrastructure should serve national and Union cybersecurity interests and needs, leveraging state of the art technology for advanced data collection and analytics tools, enhancing cyber detection and management capabilities and providing real-time situational awareness. That infrastructure should serve to increase detection of cybersecurity threats and incidents and thus complement and support Union entities and networks responsible for crisis management in the Union, notably the EU Cyber Crises Liaison Organisation Network ('EU-CyCLONe'), as defined in Directive (EU) 2022/2555 of the European Parliament and of the Council[82].

Commented [A281]: Proposed: This should be national CSIRTs.

(13) **Participation in the European ~~Cyber Shield~~ Cybersecurity Alert System should be voluntary for Member States.** Each Member State **that decides to join the European ~~Cyber Shield~~ Cybersecurity Alert System** should designate a **National** CSIRT~~SOC hub, public body at national level tasked with coordinating cyber threat detection activities in that Member State.~~ These National SOC~~s~~ **hubs** should **have** ~~act~~ as **functionalities the capacity to act as** a reference point and gateway at national level for participation in the European ~~Cyber Shield~~ **Cybersecurity Alert System** and should **be capable of detecting, aggregating and analysing data relevant to cyber threats and incidents, by using in particular state-of-the-art technologies and that would be shared appropriately with the CSIRT network in order to support the network 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 or existing national platforms 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**

Commented [A282]: This should be national csirt

Commented [A283]: What would be shared?

[82] 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).

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 ~~Cybersecurity Operations Centres ('Cross-border SOCs')~~ should be established. These should bring together National ~~SOCs hubs~~CSIRTs from at least three Member States, so that the benefits of cross-border threat detection and information sharing and management can be fully achieved. The general objective of Cross-border SOCs should be to strengthen capacities to analyse, prevent and detect cybersecurity threats and to support the production of high-quality intelligence on cybersecurity threats, notably through the sharing of **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.

(14a) A Member State selected by the European Cybersecurity Competence Centre (ECCC) following a call for expression of interest to set up a National SOC Hub or enhance the capabilities of an existing one, should jointly purchase relevant tools and infrastructures with the ECCC. Such a Member State should be eligible to receive a grant to operate the tools and infrastructures. 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 collaboration SOC Platform or enhance the capabilities of an existing one, should jointly purchase relevant tools and infrastructures with the ECCC. Such a Hosting Consortium should be eligible to receive a grant to operate the tools and infrastructures. 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 procurement procedure to purchase the relevant tools and infrastructures should be carried out jointly by the ECCC and relevant contracting authorities from the Member States selected following these calls for expressions of interest. Private entities should therefore not be eligible to participate in the calls for expression of interest to jointly purchase tools and infrastructures with the ECCC, or to receive grants to operate those tools and infrastructures. However, the Member States should have the possibility to involve private entities in the setting up, enhancement and operation of their National SOC Hubs and Cross-border ~~SOCs~~

Commented [A284]: Collaboration Platforms

Commented [A285]: Proposal: CSIRTs

Commented [A286]: The sources should be clearly specified

Commented [A287]: Collaboration platformd

Platforms in other ways which they deem appropriate, in compliance with national and Union law.

(15) At national level, the monitoring, detection and analysis of cyber threats is typically ensured by SOCs of public and private entities, in combination with CSIRTs. In addition, CSIRTs exchange information in the context of the CSIRT network, in accordance with Directive (EU) 2022/2555. The Cross-border ~~SOCs~~ should constitute a new capability that is complementary to the CSIRTs network **and will cooperate closely with it,** by pooling **data** and sharing **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 SOCs should act as a central point allowing for a broad pooling of relevant data and cyber threat intelligence, enable the spreading of threat information among a large and diverse set of actors (e.g., Computer Emergency Response Teams ('CERTs'), CSIRTs, Information Sharing and Analysis Centers ('ISACs'), operators of critical infrastructures). The information exchanged among participants in a Cross-border SOC could include data from networks and sensors, threat intelligence feeds, indicators of compromise, and contextualised information about incidents, threats and vulnerabilities. In addition, Cross-border SOCs should also enter into cooperation agreements with other Cross-border SOCs.

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

Commented [A288]: Collaboration Platforms

Commented [A289]: Add: with it (the CSIRTs Network)

Commented [A290]: Collaboration Platform

Commented [A291]: Same as above. This applies to all occurrences of "Cross-border SOC" so the comment is not repeated anymore.

Commented [A292]: If information is fed back to the CSIRTs Network, such agreements are not necessary.

~~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**~~ cause**s** ~~**and impacts** of cybersecurity~~ **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 in consultation with ENISA should be able to issue guidance in this respect.** This should make it possible to improve collective detection capacities and timely warnings to authorities and relevant entities, notably by using the latest artificial intelligence and data analytics technologies.

(20) By collecting, **correlating,** sharing and exchanging **data and information**, the European ~~Cyber Shield~~ **Cybersecurity Alert System** should enhance the Union's technological sovereignty. The pooling of high-quality curated data should also contribute to the development of advanced artificial intelligence and data analytics technologies. It should be facilitated through the connection of the European ~~Cyber Shield~~ **Cybersecurity Alert System** with the pan-European High Performance Computing infrastructure established by Council Regulation (EU) 2021/1173[83].

Commented [A293]: Too vague. Proposal: remove.

Commented [A294]: Such competence is not in the proposal, only in recitals

Commented [A295]: Proposal: remove.

Commented [A296]: This is not clear. Perhaps the entire point should be removed.

Commented [A297]: Link to HPC is not clear and article on this matter has already been deleted – proposal: remove

[…]

(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 cybersecurity incidents and complement Member States' actions through emergency financial support for preparedness, response and **initial ~~immediate~~** recovery of essential services. That instrument should enable the rapid deployment of assistance in defined circumstances and under clear conditions and allow for a careful monitoring and evaluation of how resources have been used. Whilst the primary responsibility for preventing, preparing for and responding to cybersecurity incidents and crises lies with the Member States, the Cyber Emergency Mechanism promotes solidarity between Member States in accordance with Article 3(3) of the Treaty on European Union ('TEU') and could be used to complement Member States effort.

(25) The Cyber Emergency Mechanism should provide support to Member States complementing their own measures and resources, and other existing support options in case of response to and **~~immediate~~ 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[84] **~~and Hybrid Rapid Response Teams~~**. It should address the need to ensure that specialised means are available to support preparedness and response to cybersecurity incidents across the Union and in third countries.

Commented [A298]: Is cyclone offering mitigation support ?

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

[…]

(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 ENISA ~~the Commission~~ and the affected Member State should be ensured. When requesting support under the Cyber Emergency Mechanism, the Member State should provide relevant information justifying the need for support. Such information should be provided only to ENISA.

[…]

(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 including through exercise, and training of entities operating in ~~**highly critical**~~ sectors **of high criticality** identified pursuant to Directive (EU) 2022/2555 in a coordinated manner. For this purpose, the Commission, with the support of ENISA and in cooperation with the NIS Cooperation Group established by Directive (EU) 2022/2555, should regularly identify relevant sectors or subsectors, which should be proposed ~~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[85]. The selection of sectors should also take into

Commented [A299]: Activation of the Emergency Mechanism should be allowed also for sector not identified in the risk analysis of COM but identified as at risk based on MSs own risk assessment.

[85] 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

account the Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure.

[…]

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

Commented [A300]: Not clear what does it mean.

(33) 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 or large-scale cybersecurity incidents. The EU Cybersecurity Reserve should ensure the availability and readiness of services. The services from the EU Cybersecurity Reserve should serve to support national authorities in providing assistance to affected entities operating in **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, Member States should specify the support provided to the affected entity at the national level, which should be taken into account when assessing the Member State request. **The CSIRT Network established in Directive EU 2022/2555 can advise the Commission in 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.

Commented [A301]: Not practical solution as it is difficult to get the CNW position as whole

(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 will retain the overall responsibility on the functioning of the Cyber Emergency Mechanism and shall entrust ENISA with the establishment, implementation and operationalization of the EU Cybersecurity Reserve.** ~~**,**~~ **ENISA** shall be ~~**may be**~~ **the contracting authority for those services with whose operation and administration it has been entrusted.** ~~**The procurement procedures to establish the EU**~~

(EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011

~~Cybersecurity Reserve should be conducted in accordance with Regulation EU 2018/1046.~~ **The resulting contracts, including any framework contract and specific contracts implementing a framework contract, should be signed by the contracting authority and the** ~~selected~~**trusted service provider** ~~and should specify the type of services offered~~**.** ~~**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. 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.**~~ Appropriate agreements should be established between the involved parties clarifying roles and responsaibility, protection of information via non-disclosure, and liabilities . **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.**

Commented [A302]: The whole recital in confusing and does not claridy anything.
Again we reitarate the comment to receive a clear indication who how this will work in practice, what kind of contracts will be signed, with whom and what are the rules for liability ?

[…]

(37) Taking into account the unpredictable nature of cybersecurity attacks and the fact that they are often not contained in a specific geographical area and pose high risk of spill-over, the strengthening of resilience of neighbouring countries and their capacity to respond effectively to significant and large-scale cybersecurity incidents contributes to the protection of the Union as a whole. Therefore, third countries associated to the DEP may be supported from the EU Cybersecurity Reserve, where this is provided for in the ~~**respective association**~~ **relevant** agreement **or Association Council decision through which** ~~**to**~~ **the third country is associated** to DEP. The decision to deploy the reserve should be made by the Member States. **The CSIRT Network established in Directive EU 2022/2555 can advise the Commission in reviewing requests for support from the EU Cybersecurity Reserve.**

Commented [A303]: It should be political not technical level – CYCLONe seems to advice, but decision to deploy should be made the the Councli

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**~~.

(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.

Commented [A304]: There should not be implementing acts

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

HAVE ADOPTED THIS REGULATION:

Chapter I

GENERAL OBJECTIVES, SUBJECT MATTER, AND DEFINITIONS

Article 1

Subject-matter and objectives

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

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

Commented [A305]: Support for FR proposal

[…]

Article 2

Definitions

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

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

Commented [A306]: This is superfluous and can be replaced with National CSIRTs as defined in NIS1/2.
Motivation: National CSIRTs already perform this role.

[…]

Chapter II

THE EUROPEAN ~~CYBER SHIELD~~ CYBERSECURITY ALERT SYSTEM

Article 3

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

1. An interconnected pan-European infrastructure **that consists** of ~~National SOC hubs and~~ **Cross-border ~~SOC~~ collaboration platforms joining on a voluntary basis** ~~Security Operations Centres ('European Cyber Shield~~ **the European Cybersecurity Alert System**~~')~~ shall be established to **support the** develop**ment of** advanced capabilities for the Union to detect, analyse and process data on cyber threats and incidents in the Union. ~~It shall consist of all National Security Operations Centres ('National SOCs') and Cross-border Security Operations Centres ('Cross-border SOCs').~~

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

2. The European ~~Cyber Shield~~ **Cybersecurity Alert System** shall:

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

   Commented [A307]: Support for NL comments to use the term "analysed" or "aggregated" throughout articles 3 to 8 of this act when referencing to "information" or "data".

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

   Commented [A308]: It is not necessary to mention specific 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, CSIRTs and the CSIRTs network**;

(d) contribute to **enhanced** ~~faster~~ detection of cyber threats and 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~~.

Commented [A309]: Mentioning AI here is not necessary.

~~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 CSIRTs ~~Security Operations Centres~~ ~~Hubs~~

Commented [A310]: As mentioned in comments to Article 1: this is superfluous and can be replaced with National CSIRTs as defined in NIS1/2.
Motivation: National CSIRTs already perform this role.

1. ~~In order~~ **Where a Member State decides** to **voluntarily** participate in the European ~~Cyber Shield~~ **Cybersecurity Alert System**, ~~each Member State~~ **it** shall designate at least one National CSIRT ~~SOC~~ ~~**Hub**~~. ~~The National SOC shall be a public body.~~

Commented [A311]: As a compromise proposal to address specific needs of some MS, PL support the NL proposal

~~It shall have the capacity to act as a reference point and gateway to other public and private organisations at national level for collecting and analysing information on cybersecurity threats and incidents and contributing to a Cross-border SOC. It shall be equipped with state-of-the-art technologies capable of detecting, aggregating, and analysing data relevant to cybersecurity threats and incidents.~~

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

3. A **Member State** ~~National SOC~~ selected pursuant to paragraph 2 shall commit to apply **for their National** ~~SOC hubs~~**CSIRT** to participate in a Cross-border ~~SOC~~ **collaboration Platform** within two years from the date on which the tools and infrastructures are acquired, or on which it receives grant funding, whichever occurs sooner. If a **Member State's** National ~~SOC hub~~**CSIRT** 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 ~~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 CSIRT** ~~SOC hubs~~ **or another public body, as defined in Article 2(2)work** ~~working~~ together to coordinate their cyber-detection and threat monitoring activities shall be eligible to participate in actions to establish a Cross-border SOC **collaboration Platform**.

Commented [A312]: Support for the NL proposal, but there should also be recital stating that choosing the public body should be made in exceptional case. First and foremost this should be CSIRT

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

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

4. A 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** ~~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 and infrastructures already jointly procured with that Hosting Consortium.

Article 6

Cooperation and information sharing within and between cross-border ~~SOCs~~ collaboration Platforms

1. Members of a Hosting Consortium shall **ensure that their National ~~SOC hubs~~CSIRT** exchange**, in accordance with the Consortium Agreement,** relevant information among themselves [illegible] Commented [A313]: Remove

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

   (b) enhances the level of cybersecurity of the European Union, in particular through raising awareness in relation to cyber threats, limiting or impeding the ability of such threats to spread, supporting a range of defensive capabilities, vulnerability remediation and disclosure, threat detection, containment and prevention techniques, mitigation strategies, or response and recovery stages or promoting collaborative threat research between public and private entities.

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

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

   (b) a governance framework **clarifying and** incentivising the sharing of information **referred to in paragraph 1** by all participants;

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

3. To encourage exchange of information between Cross-border ~~SOCs~~ **collaboration Platforms**, Cross-border SOC~~s~~ **collaboration Platforms** shall ensure a high level of interoperability between themselves. To facilitate the interoperability between the Cross-border ~~SOCs~~ **collaboration Platforms**, the Commission may ~~provide guidelines, with support of ENISA, by means of implementing acts, taking into account the ECCC and after consulting~~ for this interoperability. Those ~~implementing acts~~ guidelines shall be adopted in accordance with the examination procedure referred to in Article 21(2) of this Regulation. **Before submitting those draft** ~~guidelines implementing acts~~ **to the committee referred to in Article 21(1), the Commission shall consult the** ~~ECCC~~ **CSIRT Network and existing Cross-border SOC collaboration Platforms.**

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

2. ~~The Commission may, by means of implementing acts, determine the procedural arrangements for the information sharing provided for in paragraphs 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2) of this Regulation.~~ Each Cross-border collaboration platform shall ensure that they have procedural arrangements for the information sharing in paragraph 1.

Article 8

Security

[…]

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~~

Commented [A314]: The primary flow of information should be to the CSIRTs Network.

Commented [A315]: PL strong support. There should not be any implementing acts

Commented [A316]: PL strong support. There should not be any implementing acts

Commented [A317]: CSIRTs Network should be at least consulted or decide on this.

Commented [A318]: The cooperation and information sharing activities should also concern significant incidents ; As to the rest of the threats or incidents - it would be worth adding provision which allows sharing information about them voluntarily.

Commented [A319]: Very important for PL not establish separate information sharing structures. The CSIRTs Network, to which the Commission - through CERT-EU - is a member, would be the designated network to receive this information.

Commented [A320]: Pl strongly believes there should not be any implementing acts

Chapter III

CYBER EMERGENCY MECHANISM

[…]

Article 10

Type of actions

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

   (a) preparedness actions**:**~~,~~ ~~including~~

   (xiii) the coordinated preparedness testing of entities operating in **sectors of high criticality** ~~highly critical sectors~~ across the Union;

   (xiv) other preparedness actions for entities operating in sectors of high criticality ~~critical~~ and other ~~highly~~ critical sectors, including those involving exercises and trainings ~~and~~ ;

   (b) ~~response~~ actions~~,~~ supporting response to and **~~initiating~~** ~~immediate~~ recovery from significant and large-scale cybersecurity incidents, to be provided by trusted providers participating in the EU Cybersecurity Reserve established under Article 12;

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

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

Article 11

Coordinated preparedness testing of entities

1. For the purpose of supporting the voluntary coordinated preparedness testing of entities referred to in Article 10(1), point (a), across the Union, **and with due respect to the Member States competences,** the Commission, after consulting the NIS Cooperation Group and ENISA, shall identify the sectors, or sub-sectors, concerned, from the Sectors of High Criticality listed in Annex I to Directive (EU) 2022/2555 from which **Member States may**

request to participate and to this end propose entities to ~~may~~ be subject to the coordinated preparedness testing.~~,~~

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

2. The NIS Cooperation Group in cooperation with the EU-CyCLONe, ~~-~~Commission, ENISA, and the High Representative, shall develop common risk scenarios and methodologies for the **coordinated testing exercises under Article 10 (1) (a) (i). The NIS Cooperation Group, in cooperation with Commission, ENISA and the High Representative, may develop common risk scenarios and methodologies for other preparedness actions under Article 10(1)(a)(ii).**

Article 12

Establishment of the EU Cybersecurity Reserve

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

1a. At request of Member States to esure proper allocation of resource the EU Cybersecurity Reserve may be used, to provide preparedeness services to the users.

2. The EU Cybersecurity Reserve shall consist of incident response services from trusted providers selected in accordance with the criteria laid down in Article 16. The Reserve shall include pre-committed services. The ~~services~~ **Reserve shall** be deployable **upon request** in all Member States **and in third countries referred to in Article 17 (1).**

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

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

(b) ~~Union institutions, bodies and agencies.~~

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

Commented [A321]: Cybersecurity Reserve has to be practicla, well-functioning and effective.
There is still need for discussion how to make this intrument to provide real added value which was not yet possible due to the paste of negotiations
PL is strongly in favour to have this discussion in the Working Party in order be able to make the necessary amendments in the legal text. Without proper understanding it is not possible to make meanigful amendments

Formatted: Outline numbered + Level: 7 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 3.81 cm + Indent at: 4.44 cm

Formatted: Indent: Left: 0.63 cm, No bullets or numbering

Formatted: Indent: Left: 4.44 cm, First line: 0 cm

Commented [A322]: EUIBAS should not use the DEP resources , as a compromise PL can accept to indicate certEU

Commented [A323]: It should be further defined – what kinf od users ?

(d) entities operating in sectors of high criticality or other critical sectors

Commented [A324]: At the same time this is not clear, why not to refer to NIS2 or CER

5. The Commission shall ~~responsibility~~ **have** shared ~~overall~~ **responsibility** with Member States for ~~the implementation of~~ the EU Cybersecurity Reserve. **To that end, the** Commission**, in cooperation with the NIS Cooperation Group and ENISA,** shall determine the priorities and evolution of the EU Cybersecurity Reserve, in line with the requirements of the users referred to in paragraph 3, and shall supervise its implementation, and ensure complementarity, consistency, synergies and links with other support actions under this Regulation as well as other Union actions and programmes. **These priorities shall be revised every two years.**

6. The Commission ~~**may**~~ **shall** entrust the establishment, operation and administration of the EU Cybersecurity Reserve ~~, in full or in part,~~ to ENISA, by means of contribution agreements.

7. ~~In order to support the Commission in establishing the EU Cybersecurity Reserve,~~ ENISA shall prepare a mapping of the services needed **and their availability**, after consulting ~~**Member States**~~ **the NIS Cooperation Group** and the Commission. ENISA shall prepare a similar mapping, after consulting the **the NIS Cooperation Group and the** Commission, to identify the needs of third countries eligible for support from the EU Cybersecurity Reserve pursuant to Article 17. The Commission, where relevant, **may** ~~shall~~ **seek the views of** ~~**consult**~~ the High Representative.

8. The Commission in consultation with ENISA and after consulting CYCLONe 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). ~~**Before submitting those drafting implementing acts to the committee referred to in Article 21(1), the Commission may exchange advice and cooperate with the NIS Cooperation Group.**~~

9 . ENISA shall ensure confidentiality of the information shared in the course of requesting and providing the services. ENISA shall regularly report to Commission and NIS Cooperation Group on the general terms of usage of the cyber reserve.

Article 13

Requests for support from the EU Cybersecurity Reserve

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

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

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

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

   (a) appropriate information regarding the affected entity and potential impacts of the incident **on affected Member State(s) and users, including the risk of spill over to other Member State,** and the planned use of the requested support, including an indication of the estimated needs;

   (b) general 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.~~

Commented [A326]: Not necessary burden

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

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

7. ~~The Commission may carry out the tasks provided for in paragraph 1 of this Article by way of contribution agreements with the Union Cybersecurity Reserve. Those agreements shall comply with the requirements applicable to the Union Cybersecurity Reserve and with the specific rules set out in the relevant contribution agreements.~~ (20)

Article 14

Implementation of the support from the EU Cybersecurity Reserve

1. Requests for support from the EU Cybersecurity Reserve, shall be assessed by ~~the Commission, with the support of~~ ENISA ~~or as defined in contribution agreements under Article 12(6),~~ and a ~~response~~ decision shall be transmitted to the SPOC ~~users~~ referred to in Article 12(3) without delay **and in any event no later than 72 hours from the submission of the request to ensure effectiveness of the support action**.

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

   (a) the severity of the cybersecurity incident;~~aa~~

   (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 and Union institutions, bodies and agencies.

2a. The decision to provide EU Cybersecurity Reserve services shall be taken by the/ Council.

3. The EU Cybersecurity Reserve services shall be provided in accordance with specific agreements with trusted ~~between the service~~ providers ~~and the user to which the support under the EU Cybersecurity Reserve is provided.~~ Those agreements shall include liability conditions.

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

5. The Commission and ENISA shall bear no contractual liability for damages caused to third parties by the services provided in the framework of the implementation of the EU Cybersecurity Reserve.

Commented [A327]: Crucial point for PL – the Council has to have a much stronger role with regard to the deployment of the Reserve.
This requires indepth discussions

Commented [A328]: Not to exxlude a model as done now in the support action

Commented [A329]: This requires further clarification – who will bear the liability ?

6. [illegible]

7. ENISA ~~The Commission~~ shall report to the Commission and the NIS Cooperation Group, **on a regular basis and at least once per year,** about the use and the results of the support~~, on a regular basis~~.

[…]

Article 15a

ENISA together with the CYCLONe shall establish a framework for a voluntary cooperation at the EU level with companies willing to involve pro bono to deal with the large scale cybersecurity incidents and crises.

[…]

Article 17

Support to DEP-associated third countries

1. **A DEP- associated t~~T~~hird countr**~~y~~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 shall be 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 associated third countries eligible to receive services from the EU Cybersecurity Reserve shall include competent authorities such as CSIRTs and cyber crisis management authorities ~~,~~ as well essential entities as defined by national legislation

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

5. **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**, p~~P~~rior to receiving any support from the EU Cybersecurity Reserve, third countries shall provide to the Commission **~~and the High~~**

Commented [A330]: Why it is needed ? It ia an administrative burden for users

Formatted: Left

Formatted: Font: (Default) +Headings CS (Times New Roman), Not Italic

Commented [A331]: Remove

~~Representative~~ information about their cyber resilience and risk management capabilities, including at least information on national measures taken to prepare for significant or large-scale cybersecurity incidents, as well as information on responsible national entities, including CSIRTs or equivalent entities, their capabilities and the resources allocated to them. **The Commission shall share this information with the High Representative, for the purpose of facilitating the cooperation referred to in paragraph 6**. Where provisions of Articles 13 and 14 of this Regulation refer to Member States, they shall apply to third countries as set out in paragraph 1.

5a The decision to deploy cyber reserve shall be taken by the Council on the request of the Commission.

6. The Commission shall **inform the NIS Cooperation Group ~~Council~~ and cooperate~~coordinate~~** with the High Representative about the requests received and the implementation of the support granted to third countries from the EU Cybersecurity Reserve. **The Commission shall take into account the opinions of the NIS Cooperation Group and the High Representative, if such are provided.**

Article 17a) ~~15~~

Coordination with Union crisis management mechanisms

1. **~~In cases w~~Where a significant cybersecurity incident or a large-scale cybersecurity incident~~s~~ originate~~s~~ from or result~~s~~ in a disaster~~s~~ as defined in Article 4, point (1), of Decision No 1313/2013/EU[86], 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~~, 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.**

[…]

86 ~~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).~~

Chapter IV

CYBERSECURITY INCIDENT REVIEW MECHANISM

Article 18

Cybersecurity Incident Review Mechanism

1. ~~**After consulting Member States concerned, and A**~~at ~~the request of the Commission,~~ the EU-CyCLONe or the CSIRTs network, **and with the agreement of the Member States concerned,** ENISA shall review and assess threats, vulnerabilities and mitigation actions with respect to a specific significant or large-scale cybersecurity incident. Following the completion of a review and assessment of an incident, ENISA shall deliver an incident review report to the CSIRTs network, the EU-CyCLONe and the Commission to support them in carrying out their tasks, in particular in view of those set out in Articles 15 and 16 of Directive (EU) 2022/2555. ~~**Where relevant,**~~ **When an incident has an impact on a third country**, the Commission shall share the report with the High Representative.

[…]

Chapter V

FINAL PROVISIONS

Commented [A332]: Needs aligment with the changes in the previous chapters

Article 19

Amendments to Regulation (EU) 2021/694

[…]

FINLAND

Finland thanks the Presidency for the new compromise proposal. We see that the text is moving to the right direction in some parts and we thank the Presidency for taking into account the existing structures such as CSIRTs. However, we still have major concerns in some parts of the text, especially regarding the role of national legislation in information exchange in and between the Cross Border SOCs.

Please find attached our new comments on the text and also some new text proposals. Finland has proposed text revisions to clarify the **role of national security and legislation** in information exchange and in the Chapter 3 regarding the Cyber Emergency Mechanism to clarify forms of the **preparedness actions** and to include the preparedness actions to be provided by the Cybersecurity Reserve. Also some other text suggestions have been made.

Finland also informs the presidency, that the National Cyber Security Centre Finland (NCSC-FI) has endorsed the non-paper drafted by the CSIRTs among 19 other CERTs/CSIRTs/NCSCs. Finland sees that the non-paper elaborates well the terminology, tasks and differences between cyber incident response, threat detection and analysis actors in the cyber ecosystem and Finland notes that the **concerns from the operational level should be taken into account when drafting the CSOA text.**

Finland also notes, that to make sure the text fulfils its purpose and fits the needs of the MS, adequate time is needed to draft the text. We prefer quality over speed as our colleagues from NL already noted on Monday.

Please find below our further comments and explanations on the text. The new proposals/changes have been marked in this document in red.

Recitals

We thank the presidency for aligning the terminology better with the NIS2 Directive. Secondly, we thank for mentioning the existing structures in Recital 3, 7, 13. We have provided further clarification accordingly in recitals 3 and 13.

Regarding recital 15, Finland notes that the structures vary in MS and therefore the first sentence has been removed. It is also very important to state that the new SOC's will support the CSIRT's rather than create a new layer.

In regard the cooperation between the Cross Border SOC's, Finland agrees that there should be engouragement for cooperation to ensure flow of information but notes that no legal obligations should be made. (Recital 16, article 7)

Chapter 1

As Finland has stated in our written comments earlier, we reiterate that this Act should not create any obligations for MS to share any classified, confidential or sensitive information that would go beyond the national laws in this regard. We remind, that the legal base of the act does not allow the harmonization of the MS laws, and that should be clearly noted also in the text. We have provided new text proposal followingly:

Art 1(5) "All information exchange and data sharing under this Regulation shall be carried out im compliance with national rules and legislation and shall be limited to that which is relevant and

proportionate to the purpose of that exchange."

We see that the most suitable place to address this would be in the Chapter one, but we have also provided some clarifications in this regard also in other articles.

Art 2

The definitions of the SOC's needs further discussion, but to keep the definitions available for later use we have proposed the following and moved the longer descriptions in the articles 4 and 5.

(1) "National Security Operations Centre Hub' ("National SOC hub") means an entity that detects, aggregates, and analyses data relevant to cyber threats and acts as a reference point and gateway to a Cross-border SOC collaboration platform"

(2) "Cross-border Security Operations Centre collaboration Platform' ("Cross-border SOC collaboration Platform") means a multi-country platform that is designed to monitor, detect and analyse cyber threat related information »

Chapter 2

We join the concerns presented by several MS in the HWP CI regarding the issues in the SOC terminology. We also remind, that in the usual case – the role of **operations** in Security Operations Centres is the most relevant capacity of SOC's. In our understanding, the focus of the SOC's under the CSOA would focus more on the detection and analyzing of threats. Therefore, the SOC-term used in this context can be misleading. The differences between different cybert threat detection actors are well described in the CSIRT non-paper and Finland aligns with notion that the **term "national SOC" is imprecise, as it might suggest creating new operational entities.**

Secondly, as stated above, the role of national legislation should be noted in the articles 6 and 7. Therefore we have proposed several editions on those Articles to better describe the roles and responsibilities of SOC members.

In Article 8 we see, that the MS should only be responsible on the security on their part.

Chapter 3

Finland thanks the opportunity to ask questions from ENISA about their pilot project. We see the Cyber Emergency Mechanism as a continuation of the pilot project and therefore all lessons learned from ENISA are important way of improving the CSOA text.

We have suggested several changes in the whole chapter to clarify the different actions and the mechanisms behind them. The text proposed is definitely not a final one but a starting point to develop the text to better fit the needs of the MS.

To begin with, Finland notes, that preparedness, risk management, exercising and testings are the key to improve cyber resilience in the Union. The current conficts and intertwined crises have teached us, that in-time threat assesments and exercises to test our readiness may prevent cyber incidents in the future. Furthermore, we align with ENISA's view, that so called ex-ante and ex-post services should be provided together as they complement each other.

Taking that into account, **we have suggested to move article 11 and all preparedness actions to be included in the Reserve** (and provided by the trusted providers). Also the following explanation of the preparedness actions is inserted to Art 10(1a)

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

(a) preparedness actions such as coordinated preparedness testings, exercises and trainings, risk monitoring and threat assesments. The beneficiaries of these actions shall primarily be the entities operating in sectors of high criticality other critical sectors across the Union. :, including

Also several clarifications are made to differentiate the preparedness and incident response actions under the reserve.

Secondly, taking into account ENISA's tasks set out in the Cybersecurity Act and ENISA's professional capability to conduct such tasks, Finland sees that the **operation of the Cyber Emergency Mechanism should be tasked to ENISA**, not the Commission. Also, in line with that, we see it important that also ENISA is consulted when drafting the implementing acts (Art 12(8), Art 13(7)).

In assistance to third countries, instead of NIS CG, the Council should have the cooperation role. Instead of NIS CG, the CSIRT network or the CyCLONe-network could be consulted on the technical matters regarding the cyber incident.

Lastly, to ensure the complementarity of the Mechanism services, the following paragraph is inserted in Art 9(2):

2. The actions provided under the Mechanism shall complement and not replace Member States national efforts and actions to prepare for, respond to and recover from cybersecurity incidents.

Chapter 4

In this Chapter we see the text has improved and we thank the Presidency for clarifying the role of the MS in this action. However, Finland sees that the Incident Review Report should only be shared to the CSIRT network and CyCLONe – taking into account their roles in NIS2 Directive articles 15 and 16. The Commission is an observer in CyCLONe and therefore the respondent of the report in that role.

Chapter 5

Lastly, in Article 19 (2) b where derogation from the Financial Regulation is proposed, Finland notes that this is rather an **exceptional procedure** and therefore only certain activities should be allowed to derogate from the annuality principle. Due to the exceptionality of the procedure, Finland proposes to change the text accordingly:

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

[…]

Whereas:

[…]

(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[87], it is necessary to increase the resilience of citizens, businesses and entities operating critical infrastructures against the growing cybersecurity threats, which can have devastating societal and economic impacts. Therefore, investment in infrastructures and services that will support faster detection and response to cybersecurity threats and incidents is needed, and Member States need assistance in better preparing for, as well as responding to significant and large-scale cybersecurity incidents. **Building on the existing** cyber incident response **structures**, especially the CSIRTs and CSIRT network, **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.

[…]

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

(7) It is necessary to strengthen the detection and situational awareness of cyber threats and incidents throughout the Union and to strengthen solidarity by enhancing Member States' and the Union's preparedness and capabilities to respond to significant and large-scale cybersecurity incidents. Therefore a pan-European infrastructure of SOCs (European Cyber**security** ~~Shield~~ **Alert System**) should be deployed 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**, with due respect for Member State competences and without duplication of the activities conducted by the CSIRT network, EU-CyCLONe and the NIS Cooperation Group**. These actions shall be without prejudice to Articles 107 and 108 of the Treaty on the Functioning of the European Union ('TFEU').

(8) To achieve these objectives, it is also necessary to amend Regulation (EU) 2021/694 of the European Parliament and of the Council[88] 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 DEP, which aims at guaranteeing the resilience, integrity and trustworthiness of the Digital Single Market, at strengthening capacities to monitor cyber-attacks and threats and to respond to them, and at reinforcing cross-border cooperation on cybersecurity. This will be complemented by the specific conditions under which financial support may be granted for those actions should be established and the governance and coordination mechanisms necessary in order to achieve the intended objectives should be defined. Other amendments to Regulation (EU) 2021/694 should include descriptions of proposed actions under the new operational objectives, as well as measurable indicators to monitor the implementation of these new operational objectives.

[…]

(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,

---

88 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).

interconnection and potential effects in case of cyber-attacks affecting those infrastructures. A large-scale Union infrastructure of SOCs should be deployed ('the European Cyber**security** ~~Shield~~ **Alert System**'), comprising of several interoperating cross-border platforms, each grouping together several National SOCs. That infrastructure should serve national and Union cybersecurity interests and needs, leveraging state of the art technology for advanced data collection and analytics tools, enhancing cyber detection and management capabilities and providing real-time situational awareness. That infrastructure should serve to increase detection of cybersecurity threats and incidents and thus complement and support Union entities and networks responsible for crisis management in the Union, notably the EU Cyber Crises Liaison Organisation Network ('EU-CyCLONe'), as defined in Directive (EU) 2022/2555 of the European Parliament and of the Council[89].

(13) **Participation in the European ~~Cyber Shield~~ Cybersecurity Alert System should be voluntary for Member States.** Each Member State **that decides to join the European ~~Cyber Shield~~ Cybersecurity Alert System** should designate a **National SOC hub.** ~~public body at national level tasked with coordinating cyber threat detection activities in that Member State.~~ These National SOC~~s~~ **hubs** should **have** ~~act~~ as **functionalities the capacity to act as** a reference point and gateway at national level for participation in the European ~~Cyber Shield~~ **Cybersecurity Alert System** and should **be capable of detecting, aggregating and analysing data relevant to cyber threats and incidents, by using in particular state-of-the-art technologies** ~~-~~**and to cooperate and support the CSIRTs and CSIRT network in their activities.** ~~**and that would be shared appropriately with the CSIRT network in order to support the network 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** **and according to national legislation. Member States should be able** ~~**to decide**~~ **to designate an existing entity such as a CSIRT or existing national platforms to conduct the functions of National SOC hub, or if necessary 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 Cybersecurity Operations Centres ('Cross-border SOCs') should be established. These

[89] 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).

should bring together National SOCs from at least three Member States, so that the benefits of cross-border threat detection and information sharing and management can be fully achieved. The general objective of Cross-border SOCs should be to strengthen capacities to analyse, prevent and detect cybersecurity threats and to support the production of high-quality intelligence on cybersecurity threats, notably through the sharing of **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.

(14a) A Member State selected by the European Cybersecurity Competence Centre (ECCC) following a call for expression of interest to set up a National SOC Hub or enhance the capabilities of an existing one, should jointly purchase relevant tools and infrastructures with the ECCC. Such a Member State should be eligible to receive a grant to operate the tools and infrastructures. 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 collaboration SOC Platform or enhance the capabilities of an existing one, should jointly purchase relevant tools and infrastructures with the ECCC. Such a Hosting Consortium should be eligible to receive a grant to operate the tools and infrastructures. 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 procurement procedure to purchase the relevant tools and infrastructures should be carried out jointly by the ECCC and relevant contracting authorities from the Member States selected following these calls for expressions of interest. Private entities should therefore not be eligible to participate in the calls for expression of interest to jointly purchase tools and infrastructures with the ECCC, or to receive grants to operate those tools and infrastructures. However, the Member States should have the possibility to involve private entities in the setting up, enhancement and operation of their National SOC Hubs and Cross-border SOCs Platforms in other ways which they deem appropriate, in compliance with national and Union law.

(15) ~~At national level, the monitoring, detection and analysis of cyber threats is typically ensured by SOCs of public and private entities, in combination with CSIRTs. In addition,~~ CSIRTs

exchange information in the context of the CSIRT network, in accordance with Directive (EU) 2022/2555. The Cross-border SOCs should constitute ~~a new~~supporting ~~-~~capability that is complementary to the CSIRTs network **and will cooperate closely with it,** by pooling **data** and sharing **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. Information sharing should be carried out in compliance with national law.

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

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

cybersecurity incident. In this context, due regard should be paid to the national laws regarding information sharing, 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**~~ cause**s** ~~**and impacts** of cybersecurity~~ **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** may ~~**should be able to**~~ **issue guidance in this respect.** This should make it possible to improve collective detection capacities and timely warnings to authorities and relevant entities, notably by using the latest artificial intelligence and data analytics technologies.

(20) By collecting, **correlating,** sharing and exchanging **data and information**, the European ~~Cyber Shield~~ **Cybersecurity Alert System** should enhance the Union's technological sovereignty. The pooling of high-quality curated data should also contribute to the development of advanced artificial intelligence and data analytics technologies. It should be facilitated through the connection of the European ~~Cyber Shield~~ **Cybersecurity Alert System** with the pan-European High Performance Computing infrastructure established by Council Regulation (EU) 2021/1173[90].

(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 'High Representative'), should gradually develop dedicated

[90] 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).

protocols and standards to allow for cooperation with the cyber defence community, including vetting and security conditions. The development of the European Cyber**security 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.

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

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

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

(25) The Cyber Emergency Mechanism should provide support to Member States complementing their own measures and resources, and other existing support options in case of response to and **~~immediate~~ 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[91] **~~and Hybrid Rapid Response Teams~~**. It should address the need to ensure that specialised means are available to support preparedness and response to cybersecurity incidents across the Union and in third countries.

(26) This **~~instrument~~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~~**[92], **the EU Integrated Political Crisis Response Arrangements under Council Implementing Decision (EU) 2018/1993~~IPCR~~**[93] **(IPCR Arrangements),**

---

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

92 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).

93 **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.~~

Commission Recommendation 2017/1584[94] 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. 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.

[…]

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

(29) As part of the preparedness actions, to promote a consistent approach and strengthen security across the Union and its internal market, support should be provided for testing and assessing cybersecurity of entities operating in ~~highly critical~~ sectors **of high criticality** identified pursuant to Directive (EU) 2022/2555 in a coordinated manner. For this purpose,

[94] **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).**

the Commission, with the support of ENISA and in cooperation with the NIS Cooperation Group established by Directive (EU) 2022/2555, should regularly identify relevant sectors or subsectors, which should be eligible to receive financial support for coordinated testing at Union level. The sectors or subsectors should be selected from Annex I to Directive (EU) 2022/2555 ('Sectors of High Criticality'). The coordinated testing exercises should be based on common risk scenarios and methodologies. The selection of sectors and development of risk scenarios should take into account relevant Union-wide risk assessments and risk scenarios, including the need to avoid duplication, such as the risk evaluation and risk scenarios called for in the Council conclusions on the development of the European Union's cyber posture ~~to be~~ conducted by the Commission, the High Representative and the NIS Cooperation Group, in coordination with relevant civilian and military bodies and agencies and established networks, including the EU CyCLONe, as well as the risk assessment of communications networks and infrastructures requested by the Joint Ministerial Call of Nevers and conducted by the NIS Cooperation Group, with the support of the Commission and ENISA, and in cooperation with the Body of European Regulators for Electronic Communications (BEREC), the coordinated risk assessments to be conducted under Article 22 of Directive (EU) 2022/2555 and digital operational resilience testing as provided for in Regulation (EU) 2022/2554 of the European Parliament and of the Council[95]. 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**. 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.

[…]

---

95 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

(33) 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 or large-scale cybersecurity incidents. The EU Cybersecurity Reserve should ensure the availability and readiness of services. The services from the EU Cybersecurity Reserve should serve to support national authorities in providing assistance to affected entities operating in **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, Member States should specify the support provided to the affected entity at the national level, which should be taken into account when assessing the Member State request. **The CSIRT Network established in Directive EU 2022/2555 can advise the Commission in 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.

(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, ENISA may be the contracting authority for those services with whose operation and administration it has been entrusted. The procurement procedures to establish the EU Cybersecurity Reserve should be conducted in accordance with Regulation EU 2018/1046. 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 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. 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 in 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 Cyber 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 NIS Cooperation Group, the Commission should ensure that the views of Member States as regards priorities and 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.

(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, Member State(s) or EUIBAs concerned should be able to ask via the EU ~~=~~CyCLONe or~~,~~ the CSIRTs network ~~or the Commission~~ ~~**, with due respect of Member states competences**~~**,** ~~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 Member States concerned, 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

Commented [A333]: Is this necessary to be included in the recitals ?

the private sector, the review report on specific incidents should aim at assessing the causes, impacts and mitigations of an incident, after it has occurred. Particular attention should be paid to the input and lessons shared by the managed security service providers that fulfil the conditions of highest professional integrity, impartiality and requisite technical expertise as required by this Regulation. The report should be delivered and feed into the work of the EU~~=~~-CyCLONe, the CSIRTs network, ~~and~~ ENISA and the Commission. When the incident relates to a 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 as a whole. Therefore, third countries associated to the DEP may be supported from the EU Cybersecurity Reserve, where this is provided for in the ~~respective association~~ **relevant** agreement **or Association Council decision through which ~~to~~ the third country is associated** to DEP. **The CSIRT Network established in Directive EU 2022/2555 can advise the Commission in reviewing requests for support from the EU Cybersecurity Reserve.** 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~~.

(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.

[…]

HAVE ADOPTED THIS REGULATION:

Chapter I

GENERAL OBJECTIVES, SUBJECT MATTER, AND DEFINITIONS

Article 1

Subject-matter and objectives

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

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

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

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

2. This Regulation pursues the objective to strengthen solidarity at Union level **and enhance Member States cyber resilience** through **the** following specific objectives:

   […]

   (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 capacities **to handle** ~~against~~ significant or large-scale cybersecurity incidents, including by making Union cybersecurity incident response support available for third countries associated to the Digital Europe Programme ('DEP');

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

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

4. Without prejudice to Article 346 TFEU, the 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 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.

5. All information exchange and data sharing under this Regulation shall be carried out in compliance to national rules and legislation and shall be limited to that which is relevant and proportionate to the purpose of that exchange.

Article 2

Definitions

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

(-1) 'National Security Operations Centre Hub' ("National SOC hub") means an entity that detects, aggregates, and analyses data relevant to cyber threats and acts as a reference point and gateway to a Cross-border SOC collaboration platform. ~~**designated by and under the authority of a Member State, which has the following functionalities:**~~

~~**(a) it has the capacity to act as a reference point and gateway to other public and private organisations at national level for collecting and analysing information on cyber threats and incidents and contributing to a Cross-border SOC 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 Security Operations Centre collaboration Platform' ("Cross-border SOC collaboration Platform**") means a multi-country platform, ~~**established by a written consortium agreement** that brings together in a coordinated network structure Nnational SOCs **Hubs** from at least three Member States who form a Hosting Consortium, and~~ that ~~is~~

Commented [A334]: As stated earlier, these are still rather descriptions than definitions. We propose to move these descriptions into art 4-5 and add shorter definitions here. **We are happy to contribute to the discussion of the definitions of the SOC's/discuss about other possbile terms to replace « SOC » (eg. Cyber Detection Hub)**

Formatted: Point Manual

[illegible]

Commented [A335]: Longer definition moved below

~~(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[96];~~

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

(4) '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;

(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;

~~(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;~~

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

~~(11)~~ **(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.~~

Commented [A336]: moved above

Chapter II

THE EUROPEAN ~~CYBER SHIELD~~ CYBERSECURITY ALERT SYSTEM

Article 3

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

1. An interconnected pan-European infrastructure **that consists** of **National SOC hubs and Cross-border SOC collaboration platforms joining on a voluntary basis** ~~Security Operations Centres ('European Cyber Shield~~ **the European Cybersecurity Alert System**~~')~~ shall be established to **support the** develop**ment of** advanced capabilities for the Union to detect, analyse and process data on cyber threats and incidents in the Union. ~~It shall consist of all National Security Operations Centres ('National SOCs') and Cross-border Security Operations Centres ('Cross-border SOCs').~~

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

2. The European ~~Cyber Shield~~ **Cybersecurity Alert System** shall:

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

(b) **share** ~~**produce**~~ high-quality, actionable information and cyber threat intelligence, through the use of state-of-the art tools **and advanced technologies such as**~~, notably A~~**a**rtificial ~~I~~**i**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, in particular CSIRTs and the CSIRTs network designated or established pursuant to Article 8 of Directive (EU) 2022/2555,** ~~CSIRTs and the CSIRTs network~~;

(d) contribute to **enhanced** ~~faster~~ detection of cyber threats and situational awareness across the Union**, 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 Security Operations Centres ~~Hubs~~

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

(a) it has the capacity to act as a reference point and gateway to other public and private organisations at national level for collecting and analysing ~~information~~ on cyber threats and incidents and contributing to a Cross-border SOC 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;

2. ~~In order~~ **Where a Member State decides** to **voluntarily** participate in the European ~~Cyber Shield~~ **Cybersecurity Alert System**, ~~each Member State~~ **it** shall designate at least one National SOC **Hub**. ~~The National SOC shall be a public body.~~

~~It shall have the capacity to act as a reference point and gateway to other public and private organisations at national level for collecting and analysing information on cybersecurity threats and incidents and contributing to a Cross-border SOC. It shall be equipped with state-of-the-art technologies capable of detecting, aggregating, and analysing data relevant to cybersecurity threats and incidents.~~

Commented [A337]: Moved from definitions here

Formatted: Point Manual (1)

Formatted: Font: (Default) +Headings CS (Times New Roman), Bold, Not Strikethrough

3.~~2~~. Following a call for expression of interest, **Member States intending to participate in the European ~~Cyber Shield~~ Cybersecurity Alert System** ~~National SOCs~~ shall be selected by the European Cybersecurity Competence Centre ('ECCC') to **take part** ~~participate~~ in a joint procurement of tools and infrastructures with the ECCC**, in order to set up National SOC hubs or enhance capabilities of an existing one**. The ECCC may award grants to the selected **Member States** ~~National SOCs~~ to fund the operation of those tools and infrastructures. The Union financial contribution shall cover up to 50% of the acquisition costs of the tools and infrastructures, and up to 50% of the operation costs, with the remaining costs to be covered by the Member State. Before launching the procedure for the acquisition of the tools and infrastructures, the ECCC and the **Member State** ~~National SOC~~ shall conclude a hosting and usage agreement regulating the usage of the tools and infrastructures.

4.~~3~~. A **Member State** ~~National SOC~~ selected pursuant to paragraph 2 shall commit to apply **for their National SOC hubs** to participate in a Cross-border SOC **collaboration Platform** within two years from the date on which the tools and infrastructures are acquired, or on which it receives grant funding, whichever occurs sooner. If a **Member State's** National SOC **hub** is not a participant in a Cross-border SOC **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 Security Operations Centre~~s~~ collaboration Platforms

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

Formatted: Font: (Default) +Headings CS (Times New Roman), Bold

2. A Hosting Consortium consisting of at least three Member States, ~~represented by National SOCs~~, committed to **ensuring that their National SOC hubs work** ~~working~~ together to coordinate

their cyber-detection and threat monitoring activities shall be eligible to participate in actions to establish a Cross-border SOC **collaboration Platform**.

3.~~2~~. Following a call for expression of interest, a Hosting Consortium shall be selected by the ECCC to participate in a joint procurement of tools and infrastructures with the ECCC. The ECCC may award to the Hosting Consortium a grant to fund the operation of the tools and infrastructures. The Union financial contribution shall cover up to 75% of the acquisition costs of the tools and infrastructures, and up to 50% of the operation costs, with the remaining costs to be covered by the Hosting Consortium. Before launching the procedure for the acquisition of the tools and infrastructures, the ECCC and the Hosting Consortium shall conclude a hosting and usage agreement regulating the usage of the tools and infrastructures.

4.~~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.

5.~~4~~. A 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 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.**

6~~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 and infrastructures already jointly procured with that Hosting Consortium.**

Article 6

Cooperation and information sharing within ~~and between~~ cross-border SOCs~~s~~ collaboration Platforms

1. Members of a Hosting Consortium shall **ensure that their National SOC hubs** exchange**, in accordance with** union and national law ~~the Consortium Agreement~~**,** relevant

Commented [A338]: This Article requires major revision as Finland has stated earlier. We are happy to discuss our concerns in more detail.

Also, taking into account that this Act is mainly necessary to ensure the funding for SOCs in the upcoming years, this article goes beyond the absolute necessity what needs to be juridicially stated.

Commented [A339]: We reiterate that information exchange needs to be based on law as it can include confidential information. Therefore the text should clearly state that all information exchange is done according to national legislation, otherwise the text is harmonizing the MS laws and the legal base of the act does not allow that.

information among themselves within the 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 is necessary to:

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

[…]

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

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

(b) a governance framework **clarifying and** incentivising the sharing of information **referred to in paragraph 1** by all participants;

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

3. To encourage exchange of information between Cross-border SOC~~s~~ **collaboration Platforms**, Cross-border SOC~~s~~ **collaboration Platforms** shall ensure a high level of technical interoperability between themselves. To facilitate the interoperability between the Cross-border SOC~~s~~ **collaboration Platforms**, the Commission may, by means of implementing acts~~**, after consulting the ECCC,**~~ specify the technical 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 to the committee referred to in Article 21(1), the Commission shall consult the ECCC and existing Cross-border SOC collaboration Platforms.**

4. ~~Cross-border SOCs **collaboration 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. Where the Cross-border SOC~~s~~ **collaboration Platforms** obtain information relating to a potential or ongoing large-scale cybersecurity incident, they shall **ensure** ~~provide~~ **that**

Commented [A340]: The information exchange may include also confidential information, so there should be a threshold of necessity.

Commented [A341]: We have a constitutional issue with this – information exchange needs to be based on law as it can include confidential information.

Commented [A342]: Regarding this article we reiterate **that the legal base of the act does not allow the harmonization of the MS laws and therefore it should be clearly stated in the text that all information exchange will be carried out according to the national laws.**

Formatted: Font: (Default) +Headings CS (Times New Roman), Not Italic

relevant information **is provided** to **the CSIRTs network,** EU-=CyCLONe, ~~the CSIRTs network,~~ and the Commission, in view of their respective crisis management roles in accordance with Directive (EU) 2022/2555 and in accordance with applicable national law without undue delay.

2. The Commission may, by means of implementing acts, determine the technical requirements ~~procedural arrangements~~ for the information sharing provided for in paragraph**s** 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 on their part a high level of data security and physical security of the European ~~Cyber Shield~~ **Cybersecurity Alert System** infrastructure, and shall ensure that the infrastructure ~~shall be~~ **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 on their part that the sharing of 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 a Member State.

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** paragraph**s** 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.

Formatted: Font: (Default) +Headings CS (Times New Roman), Not Highlight

Commented [A343]: To be symmetrical with articles 6 and 8 – this formulation is better in light of the fact that impelementing powers should adress only techincal questions.

Commented [A344]: In this Article we remind that every MS is responsible for their own measures.

Chapter III

CYBER EMERGENCY MECHANISM

Commented [A345]: Several changes have been suggested in this chapter. We will be happy to discuss these revisions in more detail on Monday/later. Explanations for these changes are provided in our second document.

Article 9

Establishment of the Cyber Emergency Mechanism

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

8. The actions provided under the Mechanism shall complement and not replace Member States national efforts and actions to prepare for, respond to and recover from cybersecurity incidents.

Formatted: Point Manual (1), Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.63 cm + Indent at: 1.64 cm

Formatted: Font: (Default) +Headings CS (Times New Roman), Bold

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

Article 10

Type of actions

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

(a) preparedness actions such as coordinated preparedness testings, exercises and trainings, risk monitoring and threat assesments. The beneficiaries of these actions shall primarily be the entities operating in sectors of high criticality other-critical sectors across the Union. ~~:, including~~

(b) ~~response~~ actions~~,~~ supporting response to and **initiating** ~~immediate~~ recovery from significant and large-scale cybersecurity incidents, ~~to be provided by trusted providers participating in the EU Cybersecurity Reserve established under Article 12~~;

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

Formatted: Font: (Default) +Headings CS (Times New Roman), Not Bold

Formatted: Font: (Default) +Headings CS (Times New Roman), Not Bold

Formatted: Font: (Default) +Headings CS (Times New Roman), Not Bold

Formatted: Font: (Default) +Headings CS (Times New Roman), Not Bold

Formatted: Font: (Default) +Headings CS (Times New Roman), Not Bold

Formatted: Font: (Default) +Headings CS (Times New Roman), Bold, Underline

2. Member States may request to participate ~~may benefit from~~ in the actions referred to in paragraph 1 ~~upon request~~. The actions referred to in paragraph 1 and 2 shall be

provided by trusted providers participating in the EU Cybersecurity Reserve established under the Article 12 of this Regulation.

Formatted: Font: (Default) +Headings CS (Times New Roman), Not Bold

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, preparing for, responding or providing support for responding to significant or large-scale cybersecurity incidents, and ~~immediate~~ **initiate** recovery from such incidents.

2. The EU Cybersecurity Reserve shall consist of preparedness and incident response services from trusted providers selected in accordance with the criteria laid down in Article 16. The Reserve shall also include pre-committed services. The ~~services~~ **Reserve shall** be deployable **upon request** in all Member States **and in third countries referred to in Article 17 (1).**

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

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

   (b) Union institutions, bodies and agencies.

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

4. Users referred to in paragraph 3, point (a), shall use the services **granted upon their request** from the EU Cybersecurity Reserve in order to prepare for, respond or support response to and **initiate** ~~immediate~~ recovery from significant or large-scale incidents affecting entities operating in **sectors of high** critical**ity** or ~~**highly**~~ **other** critical sectors.

5. ENISA~~The Commission~~ shall have responsibility ~~**have overall responsibility**~~ for the implementation of the EU Cybersecurity Reserve. **To that end,** ENISA ~~**the** Commission,~~ **in cooperation with the NIS Cooperation Group and** the Commission, ~~**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~~

Commented [A347]: Taking into account ENISAs briefing in HWP CI on Monday, ENISA has the most relevant expertise and existing strutures to best implement the Emergency Mechanism. Also, in regards ENISAs resources planning, the roles and responsibilities should be clearly stated in the Act to ensure continuency of this service.

7. ~~In order to support the Commission in establishing the EU Cybersecurity Reserve,~~ ENISA shall prepare a mapping of the services needed **and their availability**, after consulting ~~**Member States**~~ **the NIS Cooperation Group** and the Commission. ENISA shall prepare a similar mapping, after consulting the **the NIS Cooperation Group and the** Commission, to identify the needs of third countries eligible for support from the EU Cybersecurity Reserve pursuant to Article 17. The Commission, where relevant, **may** ~~shall~~ **seek the views of** ~~**consult**~~ the High Representative.

8. The Commission may, by means of implementing acts, specify the types and the number of preparedness and 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). **Before submitting those drafting implementing acts to the committee referred to in Article 21(1), the Commission** shall ~~may~~ **exchange advice and cooperate with the NIS Cooperation Group** and ENISA**.**

Article 13 (11)

Preparedness actions

1. For the purpose of supporting the preparedness of entities referred to in Article 10(1), point (a), across the Union, **and with due respect to the Member States competences,** ENISA , after consulting the NIS Cooperation Group and the Commission, shall identify the sectors, or sub-sectors, concerned, from the Sectors of High Criticality listed in Annex I to Directive (EU) 2022/2555 from which **Member States may request to participate and to this end propose** entities to ~~may~~ be subject to the preparedness actions.

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

2. The NIS Cooperation Group in cooperation with the Commission, ENISA, and the High Representative, shall develop common risk scenarios and methodologies for the **preparedness actions under Article 10 (1) (a).**

Commented [A348]: Finland proposes to specify this Article and clarify, that also these services are to be provided by the Cyber Security Reserve and trusted providers. Also clarification is provided to clearly state that these services may be coordinated preparedness testings **or** other actions to support the preparedness of the entities.

Also, according to the briefing from ENISA in HWP CI, the so called ex-ante services are important part of enhancing the cyber resilience of the Union and should be provided together with the ex-post services.

Formatted: Font: (Default) +Headings CS (Times New Roman), Check spelling and grammar, Not Strikethrough

Article 13

Requests for support from the EU Cybersecurity Reserve

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

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

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

4. Requests for preparedness support referred to in Article 10(1), point (a) shall include information regarding the requested service, including the planned use of the requested support, including an indication of the estimated needs

5~~4~~. Member States shall inform the CSIRTs network, and where appropriate EU-CyCLONe, about their requests for for services referred to in Article 10(1), point (b), ~~incident response and **initiate** immediate recovery support pursuant to this Article.~~

(a) appropriate information regarding the affected entity and potential impacts of the incident **on affected Member State(s) and users, including the risk of spill over,** and the planned use of the requested support, including an indication of the estimated needs;

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

(c) **where relevant, available** information about other forms of support available to the affected entity, including contractual arrangements in place for incident response and **initial** ~~immediate~~ recovery services, as well as insurance contracts potentially covering such type of incident.

6~~5~~**a. 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.**

7~~6~~. ENISA, in cooperation with the Commission and the NIS Cooperation Group, shall develop a template to facilitate the submission of requests for support from the EU Cybersecurity Reserve.

87. 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). **Before submitting those drafting implementing acts to the committee referred to in Article 21(1), the Commission shall exchange advice and cooperate with ENISA.**

Formatted: Font: (Default) +Headings CS (Times New Roman), Bold, Check spelling and grammar

Article 14

Implementation of the support from the EU Cybersecurity Reserve

1. Requests for support from the EU Cybersecurity Reserve for services referred to in Article 10(1), point (b), shall be assessed by the Commission, with the support of ENISA or as defined in contribution agreements under Article 12(6), and a response shall be transmitted to the users referred to in Article 12(3) without delay **and in any event no later than 72 hours from the submission of the request to ensure effectiveness of the support action**.

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

[…]

(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 and Union institutions, bodies and agencies.

[…]

6. Within **three** one month**s** from the end of the support action for services referred to in Article 10(1), point (b), the users shall provide **the** Commission**,** and ENISA**, the CSIRTs network and, where appropiate, EU-CyCLONe** with a summary report about the service provided, results achieved and the lessons learned. When the user is from a third country as set out in Article 17, such report shall be shared with the High Representative.

7. The Commission shall report to the NIS Cooperation Group**, on a regular basis and at least once per year,** about the use and the results of the support, on a regular basis.

Article 15

Coordination with crisis management mechanisms

~~1. In cases where significant or large-scale cybersecurity incidents originate from or result in disasters as defined in Decision 1313/2013/EU[97], the support under this Regulation for responding to such incidents shall complementactions under and without prejudice to Decision 1313/2013/EU.~~

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

~~3. In consultation with the High Representative, support under the Cyber Emergency Mechanism may complement assistance provided in the context of the Common Foreign and Security Policy and Common Security and Defence Policy, including through the Cyber Rapid Response Teams. It may also complement or contribute to assistance provided by one Member State to another Member State in the context of Article 42(7) of the Treaty on the European Union.~~

~~4. Support under the Cyber Emergency Mechanism may form part of the joint response between the Union and Member States in situations referred to in Article 222 of the Treaty on the Functioning of the European Union.~~

Article 16

Trusted providers

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

   (a) ensure **that the services included in** the EU Cybersecurity Reserve **are such that the Reserve** ~~includes services that~~ may be deployed in all Member States, taking into account in particular national requirements for the provision of such services, including certification or accreditation;

   […]

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

   […]

[97] 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).

(d) the provider shall have appropriate security clearance, at least for personnel intended for service deployment~~:~~**, where required by a Member State;**

[…]

(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.

Article 17

Support to DEP-associated third countries

1. **A DEP- associated t**~~**T**~~hird country**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 shall be 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.

[…]

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**, **p**~~**P**~~rior to receiving any support from the EU Cybersecurity Reserve, third countries shall provide to the Commission ~~**and the High Representative**~~ information about their cyber resilience and risk management capabilities, including at least information on national measures taken to prepare for significant or large-scale cybersecurity incidents, as well as information on responsible national entities, including CSIRTs or equivalent entities, their capabilities and the resources allocated to them. **The**

Commission shall share this information with the High Representative, for the purpose of facilitating the cooperation referred to in paragraph 6. Where provisions of Articles 13 and 14 of this Regulation refer to Member States, they shall apply to third countries as set out in paragraph 1.

6. The Commission shall **inform the ~~NIS Cooperation Group~~ Council and cooperate~~coordinate~~** with the High Representative about the requests received and the implementation of the support granted to third countries from the EU Cybersecurity Reserve. **The Commission shall take into account the opinions of the Council ~~NIS Cooperation Group~~ and the High Representative, if such are provided.**

Formatted: Font: (Default) +Headings CS (Times New Roman), Not Strikethrough

Article 17a) ~~15~~

Coordination with Union crisis management mechanisms

1. **~~In cases w~~Where a significant cybersecurity incident or a large-scale cybersecurity incident~~s~~ originate~~s~~ from or result~~s~~ in a disaster~~s~~ as defined in Article 4, point (1), of Decision No 1313/2013/EU[98], 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~~, 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.**

~~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.~~

~~98 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).~~

Chapter IV

CYBERSECURITY INCIDENT REVIEW MECHANISM

Article 18

Cybersecurity Incident Review Mechanism

1. ~~**After consulting Member States concerned, and A**~~at the request of a ~~the~~ Member State, the Commission, the EU-CyCLONe or the CSIRTs network, **and with the agreement of the Member States concerned,** ENISA shall review and assess threats, vulnerabilities and mitigation actions with respect to a specific significant or large-scale cybersecurity incident. Following the completion of a review and assessment of an incident, ENISA shall deliver an incident review report to the CSIRTs network and, the EU-CyCLONe ~~and the Commission~~ to support them in carrying out their tasks, in particular in view of those set out in Articles 15 and 16 of Directive (EU) 2022/2555. ~~**Where relevant,**~~ **When an incident has an impact on a third country**, the Commission shall share the report with the High Representative.

Commented [A349]: The Commission is an observer in CNW and CyCLONe and recipient of the report in that role.

2. To prepare the incident review report referred to in paragraph 1, ENISA shall collaborate all relevant stakeholders, including representatives of Member States, the Commission, other relevant EU institutions, bodies and agencies, managed security services providers and users of cybersecurity services. Where appropriate, **and ~~in close cooperation~~ with the agreement 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, 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) 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 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 and Cross-border SOC~~s~~ **collaboration** platforms that contribute to situational awareness in the Union and to enhancing the cyber threat intelligence capacities of the Union';

[…]

(2) Article 9 is amended as follows:

[…]

(b) the following paragraph 8 is added:

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

[…]

(4) The following article 16a is added:

Commented [A350]: Also, according to the ECA's opinion paper published on 5.10. ECA notes, that coordinated preparedness testing of entities should be planned activities and are therefore in general neither unpredictable nor exceptional. Finland alignes with the view, such planned activities do not require a derogation from the basic principle of annuality.

Commented [A351]: Article 12 of the Financial Regulation covers *Cancellation and carry-over of appropriations*. Article 12.1 includes the main rule, which is cancellation: "*Appropriations which have not been used by the end of the financial year for which they were entered shall be cancelled, unless they are carried over in accordance with paragraphs 2 to 8.*" The main rule is, in other words, that unused appropriations will be cancelled at the end of the year, unless Article 12.2 to 12.8 regulates otherwise. **It is also worth noting that the negotiations on the Recast of the Financial Regulation are ongoing.**

Finland opposes such a change mainly for two reasons: Firstly, carrying over appropriations from one year to the next would create an effect on the national budgets of Member States. It would increase Member States' contributions to the EU budget because certain appropriations would not be decommitted. Thus, the proposed flexibility for the implementation of the EU budget would ultimately have the effect of increasing Finland's and other Member States' EU contributions.

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.

[…]

SWEDEN

[…]

(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[99], Commission Recommendation (EU) 2017/1584[100], Directive 2013/40/EU of the European Parliament and of the Council[101] and Regulation (EU) 2019/881 of the European Parliament and of the Council[102]. 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 and Member State(s) concerned, to enhance the resilience of critical infrastructure used to provide essential services in the internal market.

[…]

(7) It is necessary to strengthen the detection and situational awareness of cyber threats and incidents throughout the Union and to strengthen solidarity by enhancing Member States' and the Union's preparedness and capabilities to respond to significant and large-scale cybersecurity incidents. Therefore a pan-European infrastructure of SOCs (European Cyber**security** ~~Shield~~ **Alert System**) should be deployed 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**, with due respect for Member States national competences and without**

---

99 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).

100 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).

101 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).*

102 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).

duplication of the activities conducted by the CSIRT network, EU-CyCLONe and the NIS Cooperation Group. These actions shall be without prejudice to Articles 107 and 108 of the Treaty on the Functioning of the European Union ('TFEU').

[…]

(11) ~~For the purpose of sound financial management, specific rules should be laid down for the carry-over of unused commitment and payment appropriations. While respecting the principle that the Union budget is set annually, this Regulation should, on account of the unpredictable, exceptional and specific nature of the cybersecurity landscape, provide for possibilities to carry over unused funds beyond those set out in the Financial Regulation, thus maximising the Cybersecurity Emergency Mechanism's capacity to support Member States in countering effectively cyber threats.~~

Commented [A352]: There are already possibilities within the Financial regulation to carry over commitments and payment appropriations. Therefore, SE proposes to delete this paragraph since there is no reason to establish specific rules relating to the Cybersecurity Emergency Mechanism.

[…]

(13) **Participation in the European ~~Cyber Shield~~ Cybersecurity Alert System should be voluntary for Member States.** Each Member State **that decides to join the European ~~Cyber Shield~~ Cybersecurity Alert System** should designate a **National SOC hub.** ~~public body at national level tasked with coordinating cyber threat detection activities in that Member State.~~ These National SOC~~s~~ **hubs** should **have** ~~act~~ as **functionalities the capacity to act as** a reference point and gateway at national level for participation in the European ~~Cyber Shield~~ **Cybersecurity Alert System** and should **be capable of detecting, aggregating and analysing data relevant to cyber threats and incidents, by using in particular state-of-the-art technologies and that would be shared appropriately with the CSIRT network in order to support the network 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 or existing national platforms 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.**

Commented [A353]: We still see a risk of duplication of tasks between these proposed National SOC hubs and the national representation in the CSIRTs Network.

However, SE will send specific comments on these recitals when the corresponding articles are fully negotiated.

(14) As part of the European Cyber**security Alert System** ~~Shield~~, a number of Cross-border Cybersecurity Operations Centres ('Cross-border SOCs') should be established. These should bring together National SOCs from at least three Member States, so that the benefits of cross-border threat detection and information sharing and management can be fully achieved. The general objective of Cross-border SOCs should be to strengthen capacities to analyse, prevent and detect cybersecurity threats and to support the production of high-quality intelligence on cybersecurity threats, notably through the sharing of **information**

~~**data**~~ from various open 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 the CSIRTs Network and complementing existing SOCs ~~and computer incident response teams ('CSIRTs')~~ and other relevant actors.

[…]

(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 should be able to issue guidance in this respect.**~~ This should make it possible to improve collective detection capacities and timely warnings to authorities and relevant entities, ~~notably by using the latest~~such as artificial intelligence and data analytics technologies.

(20) By collecting, ~~**correlating,**~~ sharing and exchanging **data and information**, the European ~~Cyber Shield~~ **Cybersecurity Alert System** should enhance the Union's ~~technological~~ digital sovereignty. The pooling of high-quality curated data should also contribute to the development of advanced artificial intelligence and data analytics technologies. It should be facilitated through the connection of the European ~~Cyber Shield~~ **Cybersecurity Alert System** with the pan-European High Performance Computing infrastructure established by Council Regulation (EU) 2021/1173[103].

[103] 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).

(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 'High Representative'), should gradually develop dedicated protocols and standards to allow for cooperation with the cyber defence community, including vetting and security conditions. The development of the European Cyber**security Alert System** ~~Shield~~ should be accompanied by a gap analysis ~~reflection~~ enabling future collaboration with networks and platforms responsible for information sharing in the cyber defence community, in close cooperation with the High Representative.

Commented [A354]: MS were sceptical to wordings stating a cooperation between civilian and military SOCs when negotiating the Council conslusions on the Cyber Defence Policy.

SE is still hesitant, but will get back with specific comments when the scoop and tasks of the articles in this regulation are negotiated.

[…]

(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, ENISA may be the contracting authority for those services with whose operation and administration it has been entrusted. The procurement procedures to establish the EU Cybersecurity Reserve should be conducted in accordance with Regulation EU 2018/1046. 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 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. 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 in 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 Cyber 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 NIS Cooperation Group, the Commission should ~~ensure that the views of~~consult with Member States ~~as regards~~regarding 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.

(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' national competences,** 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 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,

Commented [A355]: We would like to ask for the rational behind this addition.

impacts and mitigations of an incident, after it has occurred. Particular attention should be paid to the input and lessons shared by the managed security service providers that fulfil the conditions of highest professional integrity, impartiality and requisite technical expertise as required by this Regulation. The report should be delivered and feed into the work of the EU=-CyCLONe, the CSIRTs network and the Commission. When the incident relates to a third country, it **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 as a whole. Such activities further contribute to the EU:s cyber diplomacy. Therefore, third countries associated to the DEP may be supported from the EU Cybersecurity Reserve, 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 CSIRT Network established in Directive EU 2022/2555 can advise the Commission in reviewing requests for support from the EU Cybersecurity Reserve.** 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**~~.

[…]

HAVE ADOPTED THIS REGULATION:

Chapter I

GENERAL OBJECTIVES, SUBJECT MATTER, AND DEFINITIONS

Article 1

Subject-matter and objectives

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

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

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

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

[…]

3. This Regulation is without prejudice to the Member States' sole ~~primary~~ responsibility for **safeguarding** national security in line with article 4.2 TEU ~~, public security,~~ **and their power to safeguard other essential State functions, including ensuring the territorial integrity of the State and maintaining law and order.** ~~and the prevention, investigation, detection and prosecution of criminal offences.~~

[…]

Article 2

Definitions

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

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

(a) it has the capacity to act as a reference point and gateway to other public and private organisations at national level for collecting and analysing ~~information~~ ~~on~~ cyber threats and incidents and contributing to a Cross-border Cyber~~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 Security Operations Centre collaboration Platform**' ("**Cross-border SOC collaboration Platform**") means a multi-country platform, **established by a written consortium agreeement** that brings together in a coordinated network structure **N~~n~~**ational SOC~~s~~ **Hubs** from at least three Member States ~~who form a Hosting Consortium~~, and that is

Commented [A356]: SE still proposes that the term SOC is to be deleted throughout the text. See some suggestions below.

Commented [A357]: SE still proposes that the term SOC is to be deleted throughout the text. In exchange SE suggests that either "Threat-intelligence sharing platform" or "National Cyber Hub" is used.

SE is flexible to other suggestions that do not have an already (quite) established definition.

Rational:
SOC is a widely used term with a somewhat coherent definition – a specific unit/group/function with specific tasks.

The COM has, on several occasions, explained that their intention with this proposal is not to specify which unit/group/function within the MSs that is to be responsible for these new tasks. Therefore, SE finds it unfortunate that the COM and the PRES insists on using a term that traditionally defins a specific unit/group/function.

This regulation proposes a new platform/tool for an unidentified unit/group/function within the MSs. Where it is the prerogative of the MSs to decide who are to be tasked with this new platform/tool.

What this regulation is proposing would give the term "SOC" a new definition, one that is not in alignment with the one widely used in the it-communities.

Commented [A358]: SE does not support the use of the term SOC here either.

Suggestion: Cross-border Cyber Collaboration Platform.

SE suggests that this is changed throughout the proposal.

designed to **monitor, detect and analyse** ~~prevent~~ cyber threats ~~and~~ **to prevent** incidents and to support the production of **cyber threat** ~~high-quality~~ intelligence, notably through the exchange of **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**;**

[…]

Chapter II

THE EUROPEAN ~~CYBER SHIELD~~ CYBERSECURITY ALERT SYSTEM

Article 3

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

1. An interconnected pan-European infrastructure **that consists** of **National SOC hubs and Cross-border SOC collaboration platforms joining on a voluntary basis** ~~Security Operations Centres ('European Cyber Shield~~ **the European Cybersecurity Alert System**~~')~~ shall be established to **support the** develop**ment of** advanced capabilities for the Union to detect, analyse and process data on cyber threats and incidents in the Union. ~~It shall consist of all National Security Operations Centres ('National SOCs') and Cross-border Security Operations Centres ('Cross-border SOCs').~~

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

2. The European ~~Cyber Shield~~ **Cybersecurity Alert System** shall:

(a) 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, CSIRTs and the CSIRTs network**;

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

(c~~b~~) produce ~~**share**~~ **produce** high-quality, actionable information and cyber threat intelligence, through the use of state-of-the art tools **and advanced technologies such**

Commented [A359]: This will be the primary task for the Cybersecurity Alert System.
SE thus suggests that this point is moved here.

as~~, notably~~ **A**~~a~~rtificial **I**~~i~~ntelligence and data analytics**, and**, on a voluntary basis, **share that information and cyber threat intelligence** ~~technologies~~;

(~~e~~) ~~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, CSIRTs and the CSIRTs network;~~

(d) contribute to **enhanced** ~~faster~~ detection of cyber threats and 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 ~~**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 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.~~

Commented [A360]: SE would like to ask the PRES for a comment on where the purpose of these hubs will be clarified, if not here.

2. Following a call for expression of interest, **Member States intending to participate in the European ~~Cyber Shield~~ Cybersecurity Alert System** ~~National SOCs~~ shall be selected by the European Cybersecurity Competence Centre ('ECCC') to **take part** ~~participate~~ in a joint procurement of tools and infrastructures with the ECCC**, in order to set up National SOC**

hubs or enhance capabilities of an existing one. The ECCC may award grants to the selected **Member States** ~~National SOCs~~ to fund the operation of those tools and infrastructures. The Union financial contribution shall cover up to 50% of the acquisition costs of the tools and infrastructures, and up to 50% of the operation costs, with the remaining costs to be covered by the Member State. Before launching the procedure for the acquisition of the tools and infrastructures, the ECCC and the **Member State** ~~National SOC~~ shall conclude a hosting and usage agreement regulating the usage of the tools and infrastructures. Such an agreement will not include any provision that the ECCC will have insight into the threat intelligence and other information stored and shared in the tools and infrastructures that are set up.

Commented [A361]: Security level of those tool and infrastructure

3. A **Member State** ~~National SOC~~ selected pursuant to paragraph 2 shall commit to apply **for their National SOC hubs** to participate in a Cross-border SOC **collaboration Platform** within two years from the date on which the tools and infrastructures are acquired, or on which it receives grant funding, whichever occurs sooner. If a **Member State's** National SOC **hub** is not a participant in a Cross-border SOC **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 ~~Security Operations Centres~~Cyber-**collaboration Platforms**

1. A Hosting Consortium consisting of at least three Member States, ~~represented by National SOCs~~, committed to **ensuring that their National SOC hubs work** ~~working~~ together to coordinate their cyber-detection and threat monitoring activities shall be eligible to participate in actions to establish a Cross-border SOC **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 and infrastructures with the ECCC. The ECCC may award to the Hosting Consortium a grant to fund the operation of the tools and infrastructures. The Union financial contribution shall cover up to 75% of the acquisition costs of the tools and infrastructures, and up to 50% of the operation costs, with the remaining costs to be covered by the Hosting Consortium. Before launching the procedure for the acquisition of the tools and infrastructures, the ECCC and the Hosting Consortium shall conclude a hosting and usage agreement regulating the usage of the tools and infrastructures.

Commented [A362]: SE would like to ask for a comment on the reason behind this threshold of union financing.

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.

[…]

Article 6

[…]

3. To encourage exchange of information between Cross-border SOC~~s~~ **collaboration Platforms**, Cross-border SOC~~s~~ **collaboration Platforms** shall ensure a high level of interoperability between themselves. To facilitate the interoperability between the Cross-border SOC~~s~~ **collaboration Platforms**, the Commission may, by means of implementing acts~~, after consulting the ECCC,~~ after consulting the ECCC and the NIS Cooperation Group, specify the conditions for this interoperability. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2) of this Regulation. Such implementing acts will be enacted without prejudice to the national security interests of Member States. ~~Before submitting those draft implementing acts to the committee referred to in Article 21(1), the Commission shall consult the ECCC and existing Cross-border SOC collaboration Platforms.~~

Commented [A363]: SE: These implementing acts needs to be further specified in this regulation.

4. Cross-border SOC~~s~~ **collaboration 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. Where the Cross-border SOC~~s~~ **collaboration Platforms** obtain information relating to a potential or ongoing large-scale cybersecurity incident, they shall **ensure** ~~provide~~ **that** relevant information **is provided** to **the CSIRTs network,** EU-~~=~~CyCLONe, ~~the CSIRTs network,~~ and the Commission, in view of their respective crisis management roles in accordance with Directive (EU) 2022/2555 without undue delay, if the incident has or is likely to have a significant impact on services and activities falling within the scope of this Regulation.

Commented [A364]: NIS2 art 16 stipulates limitations regarding the information which should be shared with COM if there is an incident. See SE suggestion for a clarification.

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

Commented [A365]: Clarification needed.
What kind of changes does the COM foresee?
This regulation should define the premises and conditions of the interoperability and information sharing.

Article 8

Security

1. Member States participating in the European ~~Cyber Shield~~ **Cybersecurity Alert System** shall ensure a high level of data and cybersecurity, 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.

[…]

Chapter III

CYBER EMERGENCY MECHANISM

Article 9

Establishment of the Cyber Emergency Mechanism

~~8.~~9. A Cyber Emergency Mechanism is established to **support** improve**ment of** the Union's resilience to ~~major~~ cyber~~security~~ threats and prepare for and mitigate, in a spirit of solidarity, the short-term impact of significant and large-scale cybersecurity incidents (the 'Mechanism').

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

Article 10

Type of actions

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

(a) preparedness actions**:**~~:~~ ~~including~~

~~(xvii)~~(xv) the coordinated preparedness testing of entities operating in **sectors of high criticality** ~~highly critical sectors~~ across the Union;

~~(xviii)~~(xvi) **other preparedness actions for entities operating in sectors of high criticality** ~~critical~~ **and other** ~~highly~~ **critical sectors, including those involving exercises and trainings and ;**

(b) ~~response~~ actions~~,~~ supporting response to and **initiating** ~~immediate~~ recovery from significant and large-scale cybersecurity incidents, to be provided by trusted providers participating in the EU Cybersecurity Reserve established under Article 12;

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

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

Article 11

Coordinated preparedness testing of entities

1. For the purpose of supporting the coordinated preparedness testing of entities referred to in Article 10(1), point (a), across the Union~~, and with due respect to the Member States competences~~**,** the Commission, after consulting the concerned Member State(s), the NIS Cooperation Group and ENISA, shall identify the sectors, or sub-sectors, concerned, from the Sectors of High Criticality listed in Annex I to Directive (EU) 2022/2555 from which **Member States may request to participate and to this end propose** entities to ~~may~~ be subject to the coordinated preparedness testing.~~,~~

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

2. The NIS Cooperation Group in cooperation with the Commission, ENISA, and the High Representative, shall develop common risk scenarios and methodologies for the **coordinated testing exercises under Article 10 (1) (a) (i). The NIS Cooperation Group, in cooperation**

with the Commission, ENISA and the High Representative, may develop common risk scenarios and methodologies for other preparedness actions under Article 10(1)(a)(ii).

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, responding or providing support for responding to significant or large-scale cybersecurity incidents, and ~~immediate~~ **initiate** recovery from such incidents.

2. The EU Cybersecurity Reserve shall consist of incident response services from trusted providers selected in accordance with the criteria laid down in Article 16. The Reserve shall include pre-committed services. The ~~services~~ **Reserve shall** be deployable ~~upon request~~ in all Member States as well as ~~and~~ **in third countries referred to in Article 17 (1), and for each Member State there shall be at least one member organisation in the Reserve with an established office that Member State.**

Commented [A366]: The review of the ENISA Cybersecurity Support Action shows that the support is more successful if delivered by an organisation that is already established in the MS.

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

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

   (b) Union ~~institutions, bodies and agencies~~entities, as defined in regulation [Cybersecurity for the EUIBAs].

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

4. Users referred to in paragraph 3, point (a), ~~shall~~ may use the services **granted upon their request** from the EU Cybersecurity Reserve in order to provide preparedness support or to respond or support response to and **initiate** ~~immediate~~ recovery from significant or large-scale incidents affecting entities operating in **sectors of high** critical**ity** or ~~**highly**~~ **other** critical sectors.

5. The Commission shall ~~responsibility~~ **have overall responsibility** for the implementation of the EU Cybersecurity Reserve. **To that end, the** Commission**,** in consultation with the Member States and **in cooperation with the NIS Cooperation Group and ENISA,** shall determine the priorities and evolution of the EU Cybersecurity Reserve, in line with the requirements of the users referred to in paragraph 3, and shall supervise its implementation,

and ensure complementarity, consistency, synergies and links with other support actions under this Regulation as well as other Union actions and programmes. **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 a mapping of the services needed **and their availability**, after consulting Member States, ~~**Member States**~~ **the NIS Cooperation Group** and the Commission. ENISA shall prepare a similar mapping, after consulting the **the NIS Cooperation Group and the** Commission, to identify the needs of third countries eligible for support from the EU Cybersecurity Reserve pursuant to Article 17. The Commission, where relevant, **may** ~~shall~~ consult~~seek the views of~~ ~~**consult**~~ the High Representative.

8. The Commission may, after consultations with the NIS Cooperation Group, 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). **Before submitting those drafting implementing acts to the committee referred to in Article 21(1), the Commission may exchange advice and cooperate with the NIS Cooperation Group.**

Article 13

Requests for support from the EU Cybersecurity Reserve

[…]

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

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

7. ~~The Commission may, by means of implementing acts, specify further the detailed arrangements for allocating the EU Cybersecurity Reserve support services.~~ Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2).

Commented [A367]: SE would like the PRES to comment on these contribution agreements.
How will they be financed?

Commented [A368]: SE: These implementing acts needs to be further specified in this regulation.

Commented [A369]: SE: These implementing acts needs to be further specified in this regulation.

Commented [A370]: SE : these arrangements need to be more specified in this regulation. If not specified, SE suggests deletion.

Article 14

Implementation of the support from the EU Cybersecurity Reserve

1. Requests for support from the EU Cybersecurity Reserve, shall be assessed by the Member States and the Commission, with the support of ENISA or as defined in contribution agreements under Article 12(6), and a response shall be transmitted to the users referred to in Article 12(3) without delay **and in any event no later than 72 hours from the submission of the request to ensure effectiveness of the support action**.

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

   (a) the severity of the cybersecurity incident;

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

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

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

   (e) the measures taken by the user to assist the response, and ~~**immediate**~~ **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 and Union institutions, bodies and agencies.

3. The EU Cybersecurity Reserve services shall be provided in accordance with specific agreements between the service provider, the concerned Member State and the user to which the support under the EU Cybersecurity Reserve is provided. Those agreements shall include liability conditions.

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

5. The Commission and ENISA shall bear no contractual liability for damages caused to third parties by the services provided in the framework of the implementation of the EU Cybersecurity Reserve.

6. Within **three** ~~one~~ month**s** from the end of the support action, the users shall provide **the** Commission**,** ~~and~~ ENISA**, the CSIRTs network and, where appropiate, EU-CyCLONe** with a summary report about the service provided, results achieved and the lessons learned.

Commented [A371]: We are wondering if the PRES could elaborate on "a response shall be transmitted". What does this entail?

Commented [A372]: SE would welcome a clarification as to why service providers (according to art 14 para 3) has contractual liabilities, while the COM and ENISA has not.

When the user is from a third country as set out in Article 17, such report shall be shared with the High Representative.

7. The Commission shall report to the NIS Cooperation Group**, on a regular basis and at least once per year,** about the use and the results of the support~~, on a regular basis~~.

[…]

Article 16

Trusted providers

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

   (a) ensure **that the services included in** the EU Cybersecurity Reserve **are such that the Reserve** ~~includes services that~~ may be deployed in all Member States and eligible third countries, 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 an agreement ~~framework~~ to protect sensitive information relating to the service, and in particular evidence, findings and reports, and is compliant with Union security rules on the protection of EU classified information;

   […]

Article 17

Support to DEP-associated third countries

1. **A DEP- associated t~~T~~hird countr~~yies~~** 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 shall be 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 associated third countries eligible to receive services from the EU Cybersecurity Reserve shall include competent authorities such as CSIRTs and cyber crisis management authorities.

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

5. **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**, **p~~P~~**rior to receiving any support from the EU Cybersecurity Reserve, third countries shall provide to the Commission **~~and the High Representative~~** information about their cyber resilience and risk management capabilities, including at least information on national measures taken to prepare for significant or large-scale cybersecurity incidents, as well as information on responsible national entities, including CSIRTs or equivalent entities, their capabilities and the resources allocated to them. **The Commission shall share this information with the High Representative, for the purpose of facilitating the cooperation referred to in paragraph 6**. Where provisions of Articles 13 and 14 of this Regulation refer to Member States, they shall apply to third countries as set out in paragraph 1.

6. The Commission shall **inform the ~~NIS Cooperation Group~~ ~~Council~~ and cooperate**~~coordinate~~ with the High Representative about the requests received and the implementation of the support granted to third countries from the EU Cybersecurity Reserve. **The Commission shall take into account the opinions of the NIS Cooperation Group and the High Representative, if such are provided.**

Commented [A373]: Support to third countries has foreign policy dimensions, therefor we support the reinstatement of the Council.

Article 17a) ~~15~~

Coordination with Union crisis management mechanisms

1. **~~In cases w~~Where a significant cybersecurity incident or a large-scale cybersecurity incident~~s~~ originate~~s~~ from or result~~s~~ in a disaster~~s~~ as defined in Article 4, point (1), of Decision No 1313/2013/EU[104], 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~~, 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.**

~~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 A**~~at the request of the Commission, the EU-CyCLONe or the CSIRTs network, **and with the ~~agreement~~ approval of the Member**

[104] ~~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).~~

States concerned, ENISA shall review and assess threats, vulnerabilities and mitigation actions with respect to a specific significant or large-scale cybersecurity incident. Following the completion of a review and assessment of an incident, ENISA shall deliver an incident review report to the CSIRTs network, the EU-CyCLONe and the Commission to support them in carrying out their tasks, in particular in view of those set out in Articles 15 and 16 of Directive (EU) 2022/2555. ~~**Where relevant,**~~ **When an incident has an impact on a third country**, the Commission shall share the report with the High Representative.

2. To prepare the incident review report referred to in paragraph 1, ENISA shall collaborate all relevant stakeholders, including representatives of Member States, the Commission, other relevant EU institutions, bodies and agencies, managed security services providers and users of cybersecurity services. Where appropriate, **and ~~in close cooperation~~ with the ~~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, vulnerabilities and lessons learned. It shall protect confidential ~~**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 actor(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.~~

[…]