Council of the European Union
General Secretariat

Interinstitutional files:
2023/0109 (COD)

Brussels, 14 November 2023

WK 14873/2023 ADD 1

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 FR (second iteration) and IT Delegations.

Contents

FRANCE

French delegation's second written comments

2023/0109 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

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

[…]

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 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

Commented [A1]: FR : With regards to the tight deadline left for comments, the remarks incorporated below should not prevent the possibility to introduce new amendements.

Commented [A2]: FR : proposal to simplify the sentence.

Commented [A3]: FR : proposal to specify that one of the objective is to strengthen the EU competitiveness

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 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.

(4) The Union has already taken a number of measures to reduce vulnerabilities and increase the resilience of critical infrastructures and entities against cybersecurity risks, in particular Directive (EU) 2022/2555 of the European Parliament and of the Council[2], Commission Recommendation (EU) 2017/1584[3], Directive 2013/40/EU of the European Parliament and of the Council[4] and Regulation (EU) 2019/881 of the European Parliament and of the Council[5]. In addition, the Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure invites Member States to take urgent and effective measures, and to cooperate loyally, efficiently, in solidarity and in a coordinated manner with each other, the Commission and other relevant public authorities as well as the entities concerned, to enhance the resilience of critical infrastructure used to provide essential services in the internal market.

(5) The growing cybersecurity risks and an overall complex threat landscape, with a clear risk of rapid spill-over of cyber incidents from one Member State to others and from a third country to the Union requires to strengthen~~ed~~ solidarity at Union level to better detect,

Commented [A4]: FR : proposal to be in accordance with the recital 2

Commented [A5]: 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.

Commented [A6]: FR : to be in compliance with NIS2, should not we refer to essential and important entities instead of critical infrastructures ?

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

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

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).

4 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).*

5 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).

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[6].

(6) The Joint Communication on the EU Policy on Cyber Defence[7] 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 [A7]: 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

Commented [A8]: FR : proposal to be aligned with the new proposal dealing with « coordinated » EU detection instead of common detection.

Commented [A9]: FR : proposal to be aligned with the new proposal aiming to deal with the enhancement of the CSIRT network capabilities.

Commented [A10]: FR : proposal that are in line with NL proposals

Commented [A11]: 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 [A12]: FR : this sentence is confusing. Proposal of clarification

Formatted: Font: Not Bold, No underline

Commented [A13]: FR ; proposal in line with recital 2.

Commented [A14]: FR : proposal in line with NL comments

Commented [A15]: FR : proposal to specify that the coordinated detection capabilities will empower the CSIRT network.

[6] 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)

[7] 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[8] 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 [A16]: 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[9].

Commented [A17]: FR : proposal in line with NL proposal

Commented [A18]: 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 [A19]: FR ; proposal in line with previous recitals.

---

[8] 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).

[9] 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 sharing 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 [A20]: FR : proposal in line with the above recitals fostering synergies between the Support Platform and the CSIRT network

Commented [A21]: 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 [A22]: 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 [A23]: 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 [A24]: FR : please see comment above. proposal in line with the proposal to avoid dealing with the wording SOC.

Commented [A25]: 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 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

Commented [A26]: FR ; proposal to deal with stakeholders instead of actors

Commented [A27]: FR :outlines that it should not concerned security and defense information

Commented [A28]: FR recalls that it is already done within the CSIRT network.
See article 15 of NIS2

Commented [A29]: FR recalls that it is a competence of the CSIRT network (please see article 15 of NIS2)

Commented [A30]: 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.

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.

Commented [A31]: FR : proposal in line with the Danish proposal to avoid duplication between the CSIRT network and the Support platform

(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.**

Commented [A32]: FR : typo proposal

(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.

Commented [A33]: FR : would it be possible to be provided more information on what it entails

Commented [A34]: 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: Not Highlight

(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[10].

(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~~

[10] 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).

~~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 [A35]: 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 [A36]: 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.

(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 [A37]: 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: 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[11] ~~**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 [A38]: 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**~~[12], **the EU Integrated Political Crisis Response Arrangements under Council Implementing Decision (EU) 2018/1993**~~**IPCR**~~[13] **(IPCR Arrangements),**

---

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

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).

13 **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[14] 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 [A39]: 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.

[14] **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[15]. 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 [A40]: 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

[15] 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 [A41]: FR : would it be possible to specify to whom do you refer to : ENISA ? COM ? the Service providers ?

Commented [A42]: FR : it clarifies the article 12 and 13 of the text

Commented [A43]: 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 [A44]: 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 [A45]: FR : it would be beneficial for MS to be informed about the specific information that will be covered by the framework contract.

Commented [A46]: 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 oo~~f 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 [A47]: 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 [A48]: 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 [A49]: 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.

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

HAVE ADOPTED THIS REGULATION:

Chapter I

GENERAL OBJECTIVES, SUBJECT MATTER, AND DEFINITIONS

Article 1

Subject-matter and objectives

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

   (a) the establishment ~~deployment~~ of a pan-European infrastructure of ~~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~~ 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**

Commented [A50]: 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 [A51]: FR : proposal to be in line with the changes proposed in the recital 7 of the REV2

Commented [A52]: FR : proposal to be in line with the changes proposed in the recital 2 of the REV2.

Commented [A53]: FR : suggestions to define what « initial recovery » means.

Commented [A54]: FR : in line with NL proposal to clarify that the assessment should correspond to the « process of responding to large scale cyber incidents »

Commented [A55]: FR : proposals to be consistent with the changes incorporated in the article 18 on the incident review mechanism

Commented [A56]: FR : please see comment on the article 1. 1. a

Commented [A57]: 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

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.**

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 developing cyber detection, analysis, and prevention and protection capabilities in a trusted environment**;**

Commented [A58]: 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 [A59]: 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 [A60]: 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) Times New Roman, 12 pt, English (United States)

Formatted: Font: (Default) Times New Roman, 12 pt, Font color: Black, English (United States)

Commented [A61]: 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

~~(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[16];~~

(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 [A62]: 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;~~

~~(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.

---

[16] 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).

(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**~~²)~~ shall be established to **support the** develop**ment of** advanced capabilities for the Union to enhance detection, analyse 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~~**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 empowering, 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 [A63]: 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 [A64]: FR : or « CTI platform » as suggested by NL

Commented [A65]: FR : wording proposal to clarify what it entails.

Commented [A66]: FR : proposal in order to be consistent with amendments incorporated in the recital 2 of the REV2.

Commented [A67]: FR : or « CTI platform »

Commented [A68]: FR : suggestion to define what « actionable » information means and the purpose ?
Usually an information is already actionable compared to data that need analysis

Commented [A69]: FR : proposal to be consistent with recital 2

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

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

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

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

Article 4

National ~~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 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~~

Commented [A70]: FR : typo

Commented [A71]: FR : proposal to be consistent with recital 7

Commented [A72]: 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.

~~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 [A73]: 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**~~**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 [A74]: FR : typo

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 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;

Commented [A75]: FR recalls that it is a competence of the CSIRT network (article 15 of NIS2)

Commented [A76]: FR recalls that it is a competence of the CSIRT network (article 15 of NIS2)

Commented [A77]: FR recalls that it is the competence of the CSIRT network (article 15 of NIS2)

Commented [A78]: 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 [A79]: FR recalls that it is the role of the CSIRT network (please see article 15 of NIS2)

(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 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.

Commented [A80]: 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 [A81]: FR considers that as the Commissioni part of CyCLONe it will also have access to the information

Commented [A82]: 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.

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. 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 [A83]: 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 [A84]: 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

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 to be provided by trusted providers for those services would have been certified following the amendment of the Cybersecurity Act (UE 2019/881) :~~;~~ ~~including~~

(i) 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;

(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

Commented [A85]: FR : suggestion to clarify « who » will conduct the preparedness actions ?

Commented [A86]: FR : proposal to include what « coordinated prespardness 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 [A87]: FR : suggestion to clarify that we refer to the Directive NIS2

Commented [A88]: 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 ?

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). 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).**

Commented [A89]: 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 ?

Commented [A90]: 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 [A91]: FR : proposal to clarify this paragraph as the initial sentence was a bit confused.

Commented [A92]: 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 [A93]: 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 [A94]: 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 [A95]: 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 ?

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 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.

Commented [A96]: 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 [A97]: FR : do you refer to third countries competent authorities ? if so, it might be usefull.

Commented [A98]: 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.

Commented [A102]: 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 [A103]: FR : NIS Cooperation group is a « policy » group and EU CyCLONe is an operational network which is suitable for the task.

Commented [A104]: 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 [A105]: FR : please see comment above.

Commented [A106]: 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.

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.

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.

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

Commented [A107]: 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.

Formatted: Font: Bold

Commented [A108]: 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 [A109]: FR : proposal to keep the sentence simple.

Commented [A110]: 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.

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. ~~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:

   (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 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.

Commented [A111]: FR : see comment above.

Formatted: Outline numbered + Level: 7 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0 cm + Indent at: 0.63 cm

Commented [A112]: 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.

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 [A113]: FR : EU CyCLONe deals with the EU Cybersecurity crisis management and then the reports will feed its work of preparedness as foreseen under NIS2

Commented [A114]: 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[17], 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

[17] 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, 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.

   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

Commented [A115]: FR : suggest to clarify who will be the contracting authority.

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. 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.

Commented [A116]: FR considers that the Council should be involved in the assessment of the request from third countries.

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 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

Commented [A117]: FR : would like to request for a scrutiny reserve and would come back with additional comments on the text.

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[18], the support provided under this Regulation for responding to such incidents 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** 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

Commented [A118]: FR : proposals to be consistent with the recitals and with the CRA.

[18] ~~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).~~

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.**

Commented [A119]: We suggest to referred to the Article 346 TFEU.

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[19] 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:

---

[19] 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).

'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.

[…]

ITALY

These comments are without prejudice to further positions the Italian National Cybersecurity Agency or other national authorities may provide on this matter.

1 General objectives, subject matter and definition

We really appreciate the new compromise text on article 1, paragraph 3, and we thank the Spanish Presidency for the efforts made and for having taken into consideration the Italian proposals.

2 European Cyber Shield

With regards to the provision to establish a European Cybersecurity Alert System (ECAS) through cross-border Security Operation Center (SOC) Platforms, we welcome the proposal, in order to identify relevant early warning that may not be detectable at MS level, and are fully invested in identifying appropriate adjustment to ensure this novel mechanism fits and synergizes with the existing EU cyber incidents and cyber crises management mechanisms. Therefore, **we would welcome clarifications on**:

1. the role of the European Cybersecurity Alert System with respect to the CSIRT Network and CyCLONe, established by Directive 2022/2555, clearly defining the differences in order to address possible overlaps and duplications, and to ensure roles consistency as well. Indeed, the framework shall clearly define the roles of each actor involved (eg., National SOC Hubs, Cross-Border SOC Platforms, CSIRTs Network, CyCLONe, etc.) promoting effective synergies among them;
2. the information flow from the European Cybersecurity Alert System toward other stakeholders, such as the CSIRT Network and CyCLONe. In this regard, the governance will have to provide technical guidance to ensure availability and harmonization of the technical collaboration means, more specifically the taxonomies, metrics and communication protocols;
3. the establishment and functioning of cross-border SOC Platforms (article 5 and following), with particular regard to the management and reporting of EU funding that can be allocated by the ECCC, and the legal representation of the coordinating SOC. As far as the Regulation proposal makes reference to a written agreement among the consortium members, it would be interesting to know if there are any indications or guidelines on this new cooperation model;
4. the designation of national SOC Hubs. Currently, article 4 suggests the possibility for the MS to indicate one or more national SOCs. In this regard, it should be clarified how the relationships and the exchange of information between Brussels and the Capitals would be structured in the presence of more national SOCs. In particular, we believe there should be a public body performing the role of a, national SOC Hub, coordinating the other national SOCs, either public and/or private, and participating to the cross-border SOC Platforms. This does not prevent the other national SOCs, either public or private, to share information with the national SOCs of other Member States bilaterally.

See proposed amendment to articles 3 and 6 in Section 5.

3 Cyber Emergency Mechanism (CEM)

With regards to the provision concerning the Cyber Emergency Mechanism, we welcome the proposal to establish this mechanism with appropriate funding in order to strengthen and enhance

MS and EU cyber resilience. In the meanwhile, we look forward to the negotiation in order to improve the governance and applicability of some of the provided instruments. Specifically, **we would see fit**:

1. an increased involvement of the CyCLONe with respect to exercise and stress testing, fully taking into consideration the crisis preparation and management role of the newly established network as outlined by the NIS2 Directive;
2. to provide supervision and control to MS (through CyCLONe and/or Council) on the support actions for MS;
3. an in-depth analysis of the lesson learned through the ENISA Cybersecurity Support Action pilot project. In this regard, we propose to explicitly state a high-level implementation of preventive and preparedness actions with a dedicated article and rebranding the Cyber Emergency Mechanism in **Cyber Resilience Mechanism (CRM)**. Moreover, it would be useful to understand how the Cybersecurity Support Action conducted by ENISA pursuant to articles 6 and 7 of the Cyber Security Act (CSA) is integrated with the trusted providers by the managed security service providers referred to in the amendments to the CSA, currently under negotiation;
4. an evaluation of the effectiveness of the proposed Cyber Reserve, considering the business model of such cybersecurity incident response providers. In this regard we believe that users enlisted in article 12, paragraph 2, can avail themselves of the services provided by trusted providers on voluntary basis and upon their request. Moreover, in article 13, paragraph 5, the request for incident response should contain only the information needed, taking into consideration the fact that it has to remain upon Member States the decision to share sensitive information. Further amendments are under consideration;
5. a comparison with similar mechanism put in place for other domains, such as Civil Protection, introducing more flexible financial support actions to encompass tools that are not being/cannot considered here, future proofing the regulation;
6. provided the Regulation proposal aims at structuring, also through relevant funds, cyber crisis management at EU level, we believe it should also address the current lack of appropriate resilient and secure communication, envisaging the establishment of a resilient and secure network(s) connecting, for instance, MS Cyber Crisis Management Authorities (within CyCLONe), MS CSIRT (within the CSIRT Network) and relevant EUIBAs. Amendment proposals in this regard are being drafted.
7. the establishment of a Cyber Emergency Fund (CyEF), as envisaged by the Council Conclusions on an EU Cyber Posture and recalled in recital (5), in which Member States invited the Commission to present a proposal.

Moreover, the provision contained in article 11 appears to be sensitive, especially due to the role reserved to the NIS Cooperation group and ENISA, to be consulted by the EC for the purpose of identifying the sectors or subsectors involved, starting from the sectors of high criticality referred to in the Annex I of Directive (EU) 2022/2555, for the choice of entities to be subjected to coordinated preparedness testing.

See proposed amendment to articles 10-14 in Section 5.

4 Incindent Review Mechanism (IRM)

Provided cyber incident and crisis management falls within the scope of national security, which is the sole responsibility of MS, we have concerns with respect to the proposed mechanism. Therefore, we propose to extend the mandate of CyCLONe to perform such activity, at the request of MS, which may also entail the support of ENISA as CyCLONe's Secretariat.
See proposed amendment to article 18 in Section 5.

5 Proposed amendments

Please find below the articles or paragraphs that were reviewed in this round of comments, with reference to the compromise text of October 2nd, 2023 (WK 12371/2023 INIT). Proposed deletion are ~~stricken red~~ and proposed addition are **bold green**. New amendments compared to the national position of the 5th of October are in **blue**.

[…]

Recitals

(12) […] That infrastructure should serve to increase detection of cybersecurity threats and **malicious events** ~~incidents~~ and thus complement and support Union entities and networks responsible for crisis management in the Union, notably the EU Cyber Crises Liaison Organisation Network ('EU-CyCLONe'), as defined in Directive (EU) 2022/2555 of the European Parliament and of the Council[1].

(13) […] 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 capable of detecting malicious events and**~~,~~ **aggregating and analysing data relevant to cyber threats and incidents, by using in particular state-of-the-art technologies. They should also** ensure that cyber threat information from public and private entities is shared and collected at national level in an effective and streamlined manner. **Member States should be able to decide to designate an existing entity such as a CSIRT or other national public bodies to conduct the functions of National SOC hub, or establish a new one. Member States should also be able to decide to designate different entities to carry out the different functionalities of the National SOC hub.**

(15) At national level, the monitoring, detection and analysis of cyber**security** threats **and events** is typically ensured by SOCs of public and private entities, in combination with CSIRTs. […] The Cross-border SOCs **Platform** should constitute a new capability that is complementary to the CSIRTs network, by pooling and sharing data on cybersecurity threats from public and private entities, enhancing the value of such data through ~~expert analysis and~~ jointly acquired

infrastructures and state of the art tools, and contributing to the development of Union capabilities and technological sovereignty.

(17) […] Therefore, in situations where Cross-border SOCs **Platforms** 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~~**, as well as an early warning to EU-CyCLONe and the Commission to enable their timely activation.** ~~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.

(20) By collecting, **analysing, correlating, enriching,** sharing and exchanging data, the European ~~Cyber Shield~~ **Cybersecurity Alert System** should enhance the Union's technological sovereignty.

[…]

Article 1

Subject-matter and objectives

[…]

3. This Regulation is without prejudice to the Member States' **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.~~"

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 function carried out by an existing entity or a new established one, designated by the Member State, which has the following competences:**

(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 security events ~~**incidents**~~ **and contributing to a Cross-border SOC platform;**

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

The National SOC hub may be embedded within the national CSIRT or other relevant public bodies. In case the functionalities of the National SOC hub are not performed by the national CSIRT, a coordination between the two functions should be ensured;

(1) '**Cross-border Security Operations Centre Platform' ("Cross-border SOC Platform")** means a multi-country platform, **established by a written consortium agreeement** that brings together in a coordinated network structure National SOCs **Hub** from at least three Member States ~~who form a Hosting Consortium~~, and that is designed to **monitor, detect and analyse** ~~prevent~~ **security events and** cyber threats, **to prevent** incidents and to support the production of ~~high-quality~~ **threat** intelligence, notably through the exchange of data ~~from various sources, public and private~~, as well as through the sharing of state-of-the-art tools and jointly developing cyber detection, analysis, and prevention and protection capabilities in a trusted environment;

[…]

Article 3

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

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

2. ~~The~~ **ECAS**~~European Cyber Shield~~ shall:

(a) provides a security event monitoring and detection service by observing technical events in networks and systems, thus contributing to an early identification of cyber incidents by relevant entities such as competent authorities designated or established pursuant to Article 8 of Directive (EU) 2022/2555, CSIRTs and the CSIRTs network, through the analysis of the security events detected;

(b) collect, analyse, correlate and enrich data from multiple sources, such as network traffic, log files, and threat intelligence feeds with sighting information and evaluation of the overall impact of identified threats at EU level, thus providing support to strengthen the capabilities offered by the CSIRTs network and EU-CyCLONe;

(c) contribute to joint situational awareness across the Union, by producing high-quality actionable information through the use of the most advanced data analysis technologies;

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

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

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

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

(~~e~~**d**) 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.

Article 6

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

1. Members of a Hosting Consortium shall **ensure that their National SOC hubs** exchange**, in accordance with the Consortium Agreement,** relevant information among themselves within the Cross-border SOC **Platform** including information relating to **current and emerging** cyber threats, **security events,** near misses, vulnerabilities, **tactics,** techniques and procedures **used by malicious actors**, indicators of compromise, ~~adversarial tactics,~~ ~~threat-actor-specific information~~, cybersecurity alerts and recommendations regarding the configuration of cybersecurity tools to detect cyber attacks, where such information sharing:

(a) aims to prevent~~,~~ **and** detect, ~~respond to or recover~~ ~~from~~ **cyber** incidents **and** ~~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.

[…]

Article 7

Cooperation and information sharing with Union entities

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

2. Cross border SOC Platforms and the CSIRTs network shall agree on procedural arrangements and cooperate and share information on the basis thereof.
~~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.~~

Chapter III

CYBER RESILIENCE ~~EMERGENCY~~ MECHANISM

Article 9

Establishment of the Cyber Resilience ~~Emergency~~ Mechanism

1. A Cyber **Resilience** ~~**Emergency**~~ Mechanism is established to improve the Union's resilience to major cybersecurity threats and prepare for and mitigate, in a spirit of solidarity, the short-term impact of significant and large-scale cybersecurity incidents (the 'Mechanism').
2. Actions implementing the Cyber **Resilience** ~~**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 **and prevention** actions**:**, ~~including~~

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

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

[…]

(d) establishment of a Cyber Emergency Fund (CyEF) to switftly provide direct financial support to Member States necessary for their response to significant and large-scale cybersecurity incidents.

Article 10b

Cyber Resilience Mechanism Board

1. The Cyber Resilience Mechanism Board (CRMB) is composed of representatives of the Council, as chair, the Commission and the EU-CyCLONe.

2. The CRMB shall have overall responsibility for the implementation of the Cyber Resilience Mechanism (CRM), including preparedness and prevention actions, response actions, also through the EU Cybersecurity Reserve, as well as the Cyber Emergency Fund (CyEF)

3. ENISA shall provide the secretariat of the CRMB.

4. The CRMB can task the Commission, the EU-CyCLONe and ENISA to perform activities that are required to implement and enact the Cyber Resilience Mechanism (CRM).

5. The CRMB provides non biding advices in the allocation of DEP fundings concerning the actions under the Cyber Resilience Mechanism (CRM).

Article 11

Coordinated preparedness testing of entities

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

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

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

Article 11b

Establishment of a Cyber Prepardness and Prevention Program (CPPP)

1. A Cyber Prepardness and Prevention Program (CPPP) shall be established in order to assist users referred to in paragraph 3, in preparing and preventing the occurrence of significant or large-scale cybersecurity incidents.

2. The services from the Cyber Prepardness and Prevention Program (CPPP) shall be deployable in all Member States.

3. Users of the services from the Cyber Prepardness and Prevention Program (CPPP) shall include:

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

(b) Union institutions, bodies and agencies.

4. Member States' cyber crisis management authorities as referred to in Article 9 (1) and (2) of Directive (EU) 2022/2555, may use services from the Cyber Prepardness and Prevention Program (CPPP) to support essential and important entities under the Directive (EU) 2022/2555.

5. The CRMB shall have overall responsibility for the implementation of the Cyber Prepardness and Prevention Program (CPPP). The CRMB shall determine the priorities and evolution of the Cyber Prepardness and Prevention Program (CPPP), in line with the requirements of the users referred to in paragraphs 3 and 4, and shall supervise its implementation, and ensure complementarity, consistency, synergies and links with other support actions under this Regulation as well as other Union actions and programmes.

6. The CRMB shall draft a yearly program of service delivery fro the users referred to in paragraphs 3 and 4, on the basis of the requests from Member States and the Commission.

7. The CRMB may entrust the operational supervision of the Cyber Prepardness and Prevention Program (CPPP), in full or in part, to the EU-CyCLONe.

8. The CRMB, with the support of the Commission, may entrust the operation and administration of the Cyber Prepardness and Prevention Program (CPPP), in full or in part, to ENISA, by means of contribution agreements.

9. The CRMB shall prepare a mapping of the services needed and their availability, after consulting Member States.

10. At the request of the CRMB, the Commission may, by means of implementing acts, specify the types and the number of response services required for the Cyber Prepardness and Prevention Program (CPPP). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2).

Article 12

Establishment of the EU Cybersecurity Reserve

[…]

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~~ **can be deployed** in all Member States.

[…]

5. The **CRMB** ~~Commission~~ shall have overall responsibility for the implementation of the EU Cybersecurity Reserve. The **CRMB** ~~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.

5a. The CRMB may entrust the operational supervision of the EU Cybersecurity Reserve, in full or in part, to the EU-CyCLONe.

6. The **CRMB, with the support of the** Commission may**,** entrust the operation and administration of the EU Cybersecurity Reserve, in full or in part, to ENISA, by means of contribution agreements.

7. ~~In order to support the Commission in establishing the EU Cybersecurity Reserve,~~ **CRMB** ~~ENISA~~ shall prepare a mapping of the services needed **and their availability**, after consulting Member States ~~and the Commission~~. ENISA shall prepare a similar mapping, after consulting the Commission, to identify the needs of third countries eligible for support from the EU Cybersecurity Reserve pursuant to Article 17. The Commission, where relevant, shall consult the High Representative.

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

Article 13

Requests for support from the EU Cybersecurity Reserve

[…]

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

3. Requests for support from users referred to in Article 12(3), point (a), of this Regulation shall be transmitted to the **CRMB** ~~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~~ **and** 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 **type of** 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;

[…]

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

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

Article 14

Implementation of the support from the EU Cybersecurity Reserve

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

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

(a) the severity of the cybersecurity incident;

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

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

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

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

[…]

5. The **CRMB,** 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 from the end of the support action, the users shall provide **CRMB** ~~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 **CRMB** ~~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 14b

Cyber Emergency Fund (CyEF)

1. A Cyber Emergency Fund for Cybersecurity shall be established to rapidly cover immediate costs of Member States necessary for their swift response to significant and large-scale cybersecurity incidents or threats.

2. Member States may chose to avail themseleves of the Cyber Prepardness and Prevention Program (CPPP), Cybersecurity Reserve or of the Cyber Emergency Fund (CyEF).

3. The Commission shall take the necessary measure acting upon the Council conclusion on an EU Cyber Posture.

Comment: The need to establish a Cyber Emergency Fund in order to recover from immediate costs incurred by Member States acting to rapidly respond to significant and large-scale cybersecurity incidents, should be stressed and recognized in the CSoA, at least until the adoption of EU certification scheme for managed security services.

Therefore, the sole invitation, provided for in Recital 5 of the CSoA, to the Commission to present a proposal of an Emergency Fund in line with the Council conclusion on an EU Cyber Posture, could be not sufficient.

Article 18

Cybersecurity Incident Review Mechanism

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

1b. The EU-CyCLONe shall update its rules of procedures to define the process to prepare and draft the incident review report.

2. To prepare the incident review report referred to in paragraph 1, **EU-CyCLONe** ~~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. **During these activities, where appropriate and in close cooperation with the Member State(s) concerned**, **EU-CYCLONe** ~~**and in close cooperation with the Member State(s) concerned,** ENISA shall~~ **may** also collaborate with entities affected by ~~significant or~~ large-scale cybersecurity incidents. **To support the review, EU-CyCLONe** ~~ENISA~~ **may also consult other types of stakeholders.** Consulted representatives shall disclose any potential conflict of interest.

2b. Consultation and collaboration with national entities mentioned in paragraph 2 are performed through the relevant Member States' cyber crisis management authorities, established by article 9, paragraph 1, of the Directive (EU) 2555/2022.

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. **Information contained in the report shall be anonymised.** It shall protect confidential information, in accordance with Union or national law concerning the protection of sensitive or classified information.

[…]
