168644/EU XXVII. GP
Eingelangt am 10/01/24

Council of the
European Union

Brussels, 10 January 2024
(OR. en)

5315/24

Interinstitutional File:
2023/0109(COD)

CYBER 3
TELECOM 7
CADREFIN 6
FIN 35
BUDGET 3
IND 21
JAI 41
MI 27
DATAPROTECT 7
RELEX 23
CODEC 52

NOTE

From:	General Secretariat of the Council
To:	Delegations
Subject:	Proposal for a Regulation of the European Parliament and of the Coucil laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents - 4-column table

Delegations will find in the Annex a four-column table concerning the above legislative proposal, which contains:

- the Commission proposal of 18 April 2023,

- the amendments adopted by the European Parliament on 11 January 2024, and

- the Council mandate approved on 20 Decembery 2023

.

www.parlament.gv.at

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

2023/0109(COD)

	Commission Proposal	EP Mandate	Council Mandate
Formula			
1	2023/0109 (COD)	2023/0109 (COD)	2023/0109 (COD)
Proposal Title			
2	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	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	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
Formula			
3	THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,	THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,	THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
Citation 1			
4	Having regard to the Treaty on the Functioning of the European Union, and in particular Article 173(3) and Article 322(1), point (a) thereof,	Having regard to the Treaty on the Functioning of the European Union, and in particular Article 173(3) and Article 322(1), point (a) thereof,	Having regard to the Treaty on the Functioning of the European Union, and in particular Article 173(3) and Article 322(1), point (a) thereof,
Citation 2			
5	Having regard to the proposal from the European Commission,	Having regard to the proposal from the European Commission,	Having regard to the proposal from the European Commission,
Citation 3			
6	After transmission of the draft legislative act to the national parliaments,	After transmission of the draft legislative act to the national parliaments,	After transmission of the draft legislative act to the national parliaments,
Citation 4			
7	Having regard to the opinion of the Court of Auditors[1] _____ 1. OJ C […], […], p. […].	Having regard to the opinion of the Court of Auditors[1] _____ 1. OJ C […], […], p. […].	Having regard to the opinion of the Court of Auditors[1] _____ 1. OJ C […], […], p. […].
Citation 5			
8	Having regard to the opinion of the European Economic and Social Committee[1], _____	Having regard to the opinion of the European Economic and Social Committee[1], _____	Having regard to the opinion of the European Economic and Social Committee[1], _____

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
	1. OJ C , , p. .	1. OJ C , , p. .	1. OJ C , , p. .
Citation 6			
9	Having regard to the opinion of the Committee of the Regions[1], _____ 1. OJ C , , p. .	Having regard to the opinion of the Committee of the Regions[1], _____ 1. OJ C , , p. .	Having regard to the opinion of the Committee of the Regions[1], _____ 1. OJ C , , p. .
Citation 7			
10	Acting in accordance with the ordinary legislative procedure,	Acting in accordance with the ordinary legislative procedure,	Acting in accordance with the ordinary legislative procedure,
Formula			
11	Whereas:	Whereas:	Whereas:
Recital 1			
12	(1) The use of and dependence on information and communication technologies have become fundamental aspects in all sectors of economic activity as our public administrations, companies and citizens are more interconnected and interdependent across sectors and borders than ever before.	(1) The use of and dependence on information and communication technologies have become fundamental aspects***, but have, simultaneously introduced possible vulnerabilities,*** in all sectors of economic activity ***and democracy*** as our public administrations, companies and citizens are more interconnected and interdependent across sectors and borders than	(1) The use of and dependence on information and communication technologies have become fundamental aspects in all sectors of economic activity as our public administrations, companies and citizens are more interconnected and interdependent across sectors and borders than ever before.

www.parlament.gv.at

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

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
		within any specific geographical area, and occurring simultaneously or spreading instantly across many countries. ***Close and coordinated cooperation is therefore needed between the public sector, the private sector, academia, civil society and the media. Moreover, the Union's response needs to be coordinated with international institutions as well as trusted and like-minded international partners. Trusted and like-minded international partners are countries that share the Union's values of democracy, commitment to human rights, effective multilateralism, and rules-based order, in line with the international cooperation frameworks and agreements. To ensure cooperation with trusted and like-minded international partners and protection against systemic rivals, entities established in third countries that are not parties to the GPA should not be allowed to participate in procurement under this Regulation.***	many countries.
Recital 3			
14	(3) It is necessary to strengthen the competitive position of industry and services sectors in the Union across the digitised economy and support their digital transformation, by reinforcing the level of cybersecurity in the Digital Single Market. As recommended in three different proposals of the Conference on the Future of Europe[1] , it is necessary to increase the resilience of citizens, businesses and entities	(3) It is necessary to strengthen the competitive position of industry and services sectors in the Union across the digitised economy and support their digital transformation, by reinforcing the level of cybersecurity in the Digital Single Market. As recommended in three different proposals of the Conference on the Future of Europe[1] ,– it is necessary to increase the resilience of citizens, businesses***, in particular***	(3) It is necessary to strengthen the competitive position of industry and services sectors in the Union across the digitised economy and support their digital transformation, by reinforcing the level of cybersecurity in the Digital Single Market. As recommended in three different proposals of the Conference on the Future of Europe[1]-,– it is necessary to increase the resilience of citizens, businesses and entities

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
	operating critical infrastructures against the growing cybersecurity threats, which can have devastating societal and economic impacts. Therefore, investment in infrastructures and services that will support faster detection and response to cybersecurity threats and incidents is needed, and Member States need assistance in better preparing for, as well as responding to significant and large-scale cybersecurity incidents. The Union should also increase its capacities in these areas, notably as regards the collection and analysis of data on cybersecurity threats and incidents. _____ 1. https://futureu.europa.eu/en/	***microenterprises, small and medium-sized enterprises (SMEs) including startups*** -and entities operating critical infrastructures, ***including local and regional authorities*** against the growing cybersecurity threats, which can have devastating societal and economic impacts. Therefore, investment in infrastructures and services ***and building capabilities to develop cybersecurity skills*** that will support faster detection and response to cybersecurity threats and incidents is needed, and Member States need assistance in better preparing for, as well as responding to significant and large-scale cybersecurity incidents. The Union should also increase its capacities in these areas, notably as regards the collection and analysis of data on cybersecurity threats and incidents. _____ 1. ***[1]*** https://futureu.europa.eu/en/	operating critical infrastructures against the growing cybersecurity threats, which can have devastating societal and economic impacts. Therefore, investment in infrastructures and services that will support faster detection and response to cybersecurity threats and incidents is needed, and Member States need assistance in better preparing for, as well as responding to **and initial recovery from** significant and large-scale cybersecurity incidents. **Building on the existing structures and in close cooperation with them,** the Union should also increase its capacities in these areas, notably as regards the collection and analysis of data on cybersecurity threats and incidents. _____ 1. https://futureu.europa.eu/en/
Recital 3a			
14a		***(3a) Cyberattacks are frequently targeted at local, regional or national public services and infrastructures. Local authorities are among the most vulnerable targets of cyberattacks due to their lack of financial and human resources. It is therefore particularly important that decision-makers at local level are made aware of the need to increase digital resilience, increase their capacity to reduce the impact of cyberattacks and seize the***	

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
		opportunities provided for by this Regulation.	
Recital 4			
G 15	(4) The Union has already taken a number of measures to reduce vulnerabilities and increase the resilience of critical infrastructures and entities against cybersecurity risks, in particular Directive (EU) 2022/2555 of the European Parliament and of the Council[1], Commission Recommendation (EU) 2017/1584[2], Directive 2013/40/EU of the European Parliament and of the Council[3] and Regulation (EU) 2019/881 of the European Parliament and of the Council[4]. In addition, the Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure invites Member States to take urgent and effective measures, and to cooperate loyally, efficiently, in solidarity and in a coordinated manner with each other, the Commission and other relevant public authorities as well as the entities concerned, to enhance the resilience of critical infrastructure used to provide essential services in the internal market. __________ 1. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (OJ L 333, 27.12.2022). 2. Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale	(4) The Union has already taken a number of measures to reduce vulnerabilities and increase the resilience of critical infrastructures and entities against cybersecurity risks, in particular Directive (EU) 2022/2555 of the European Parliament and of the Council[1], Commission Recommendation (EU) 2017/1584[2], Directive 2013/40/EU of the European Parliament and of the Council[3] and Regulation (EU) 2019/881 of the European Parliament and of the Council[4]. In addition, the Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure invites Member States to take urgent and effective measures, and to cooperate loyally, efficiently, in solidarity and in a coordinated manner with each other, the Commission and other relevant public authorities as well as the entities concerned, to enhance the resilience of critical infrastructure used to provide essential services in the internal market. __________ 1. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (OJ L 333, 27.12.2022). 2. Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale	(4) The Union has already taken a number of measures to reduce vulnerabilities and increase the resilience of critical infrastructures and entities against cybersecurity risks, in particular Directive (EU) 2022/2555 of the European Parliament and of the Council[1], Commission Recommendation (EU) 2017/1584[2], Directive 2013/40/EU of the European Parliament and of the Council[3] and Regulation (EU) 2019/881 of the European Parliament and of the Council[4]. In addition, the Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure invites Member States to take urgent and effective measures, and to cooperate loyally, efficiently, in solidarity and in a coordinated manner with each other, the Commission and other relevant public authorities as well as the entities concerned, to enhance the resilience of critical infrastructure used to provide essential services in the internal market. __________ 1. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (OJ L 333, 27.12.2022). 2. Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale G

www.parlament.gv.at

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
	cybersecurity incidents and crises (OJ L 239, 19.9.2017, p. 36). 3. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (J L 218, 14.8.2013, p. 8). 4. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15).	cybersecurity incidents and crises (OJ L 239, 19.9.2017, p. 36). 3. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (J L 218, 14.8.2013, p. 8). 4. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15).	cybersecurity incidents and crises (OJ L 239, 19.9.2017, p. 36). 3. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (J L 218, 14.8.2013, p. 8). 4. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15).
Recital 5			
16	(5) The growing cybersecurity risks and an overall complex threat landscape, with a clear risk of rapid spill-over of cyber incidents from one Member State to others and from a third country to the Union requires strengthened solidarity at Union level to better detect, prepare for and respond to cybersecurity threats and incidents. Member States have also invited the Commission to present a proposal on a new Emergency Response Fund for Cybersecurity in the Council Conclusions on an EU Cyber Posture[1]. __________ 1. Council conclusions on the development of the European Union's cyber posture approved by the Council at its meeting on 23 May 2022, (9364/22)	(5) The growing cybersecurity risks and an overall complex threat landscape, with a clear risk of rapid spill-over of cyber incidents from one Member State to others and from a third country to the Union requires strengthened solidarity at Union level to better detect, prepare for***, respond to, and recover from,*** ~~and respond to~~ cybersecurity threats and incidents. Member States have also invited the Commission to present a proposal on a new Emergency Response Fund for Cybersecurity in the Council Conclusions on an EU Cyber Posture[1]. __________ 1. *[1]* Council conclusions on the development of the European Union's cyber posture approved by the Council at its meeting on 23 May 2022, (9364/22)	(5) The growing cybersecurity risks and an overall complex threat landscape, with a clear risk of rapid spill-over of cyber incidents from one Member State to others and from a third country to the Union requires ~~strengthened~~**to strengthen** solidarity at Union level to better detect, prepare for and respond to cybersecurity threats and incidents**, in particular by reinforcing the capabilities of existing structures such as the CSIRTs network**. Member States have also invited the Commission to present a proposal on a new Emergency Response Fund for Cybersecurity in the Council Conclusions on an EU Cyber Posture[1]. __________ 1. 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)

	Commission Proposal	EP Mandate	Council Mandate
Recital 6			
17	(6) The Joint Communication on the EU Policy on Cyber Defence[1] adopted on 10 November 2022 announced an EU Cyber Solidarity Initiative with the following objectives: strengthening of common EU detection, situational awareness and response capabilities by promoting the deployment of an EU infrastructure of Security Operations Centres ('SOCs'), supporting gradual building of an EU-level cybersecurity reserve with services from trusted private providers and testing of critical entities for potential vulnerabilities based on EU risk assessments. _____ 1. Join Communication to the European Parliament and the Council EU Policy on Cyber Defence JOIN/2022/49 final	(6) The Joint Communication on the EU Policy on Cyber Defence[1] adopted on 10 November 2022 announced an EU Cyber Solidarity Initiative with the following objectives: strengthening of common EU detection, situational awareness and response capabilities by promoting the deployment of an EU ~~*infrastructure*~~***network*** of Security Operations Centres ('SOCs'), supporting gradual building of an EU-level cybersecurity reserve with services from trusted private providers and testing of critical entities for potential vulnerabilities based on EU risk assessments. _____ 1. ***[1]*** Join Communication to the European Parliament and the Council EU Policy on Cyber Defence JOIN/2022/49 final	(6) The Joint Communication on the EU Policy on Cyber Defence[1] adopted on 10 November 2022 announced an EU Cyber Solidarity Initiative with the following objectives: strengthening of common EU detection, situational awareness and response capabilities by promoting the deployment of an EU infrastructure of Security Operations Centres ('SOCs'), supporting gradual building of an EU-level cybersecurity reserve with services from trusted private providers and testing of critical entities for potential vulnerabilities based on EU risk assessments. _____ 1. Join Communication to the European Parliament and the Council EU Policy on Cyber Defence JOIN/2022/49 final
Recital 7			
18	(7) It is necessary to strengthen the detection and situational awareness of cyber threats and incidents throughout the Union and to strengthen solidarity by enhancing Member States' and the Union's preparedness and capabilities to respond to significant and large-scale cybersecurity incidents. Therefore a pan-European infrastructure of SOCs (European Cyber Shield) should be deployed to build and enhance common detection and situational awareness capabilities; a Cybersecurity	(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 ***prevent and*** respond to significant and large-scale cybersecurity incidents. Therefore a pan-European ~~*infrastructure of*~~ ***network of*** SOCs (European Cyber Shield) should be deployed to build and enhance common detection and situational	(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**, large-scale and large-scale-equivalent** ~~and large-scale~~ cybersecurity incidents. Therefore a pan-European infrastructure of ~~SOCs~~ **Cyber Hubs** (European ~~Cyber Shield~~**Cybersecurity Alert System**) should be ~~deployed~~ **established** to

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
	Emergency Mechanism should be established to support Member States in preparing for, responding to, and immediately recovering from significant and large-scale cybersecurity incidents; a Cybersecurity Incident Review Mechanism should be established to review and assess specific significant or large-scale incidents. These actions shall be without prejudice to Articles 107 and 108 of the Treaty on the Functioning of the European Union ('TFEU').	awareness capabilities, ***reinforcing the Union's threat detection and information sharing capabilities***; a Cybersecurity Emergency Mechanism should be established to support Member States in preparing for, responding to, and immediately recovering from significant and large-scale cybersecurity incidents; a Cybersecurity Incident Review Mechanism should be established to review and assess specific significant or large-scale incidents. These actions shall be without prejudice to Articles 107 and 108 of the Treaty on the Functioning of the European Union ('TFEU').	build ~~and enhance common~~ **coordinated** detection and situational awareness capabilities; a Cybersecurity Emergency Mechanism should be established to support Member States **upon their request** in preparing for, responding to, and ~~immediately~~ **initially** recovering from significant and large-scale cybersecurity incidents; a Cybersecurity Incident Review Mechanism should be established to review and assess specific significant or large-scale incidents**. The actions under this Regulation should be conducted with due respect for Member States' competences and should complement and not duplicate the activities conducted by the CSIRT network, EU-CyCLONe and the NIS Cooperation Group, established in Directive (EU) 2022/2555**. These actions shall be without prejudice to Articles 107 and 108 of the Treaty on the Functioning of the European Union ('TFEU').
Recital 8			
19	(8) To achieve these objectives, it is also necessary to amend Regulation (EU) 2021/694 of the European Parliament and of the Council[1] in certain areas. In particular, this Regulation should amend Regulation (EU) 2021/694 as regards adding new operational objectives related to the European Cyber Shield and the Cyber Emergency Mechanism under Specific Objective 3 of DEP, which aims at guaranteeing the resilience, integrity and	(8) To achieve these objectives, it is also necessary to amend Regulation (EU) 2021/694 of the European Parliament and of the Council[1] in certain areas. In particular, this Regulation should amend Regulation (EU) 2021/694 as regards adding new operational objectives related to the European Cyber Shield and the ~~Cyber~~***Cybersecurity*** Emergency Mechanism under Specific Objective 3 of DEP, which aims at guaranteeing the resilience, integrity	(8) To achieve these objectives, it is also necessary to amend Regulation (EU) 2021/694 of the European Parliament and of the Council[1] in certain areas. In particular, this Regulation should amend Regulation (EU) 2021/694 as regards adding new operational objectives related to the European ~~Cyber Shield~~**Cybersecurity Alert System** and the Cyber Emergency Mechanism under Specific Objective 3 of **the Digital Europe Programme**

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
	trustworthiness of the Digital Single Market, at strengthening capacities to monitor cyber-attacks and threats and to respond to them, and at reinforcing cross-border cooperation on cybersecurity. This will be complemented by the specific conditions under which financial support may be granted for those actions should be established and the governance and coordination mechanisms necessary in order to achieve the intended objectives should be defined. Other amendments to Regulation (EU) 2021/694 should include descriptions of proposed actions under the new operational objectives, as well as measurable indicators to monitor the implementation of these new operational objectives. _____ 1. Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240 (OJ L 166, 11.5.2021, p. 1).	and trustworthiness of the Digital Single Market, at strengthening capacities to monitor cyber-attacks and threats and to respond to them, and at reinforcing cross-border cooperation on cybersecurity. This will be complemented by the specific conditions under which financial support may be granted for those actions should be established and the governance and coordination mechanisms necessary in order to achieve the intended objectives should be defined. Other amendments to Regulation (EU) 2021/694 should include descriptions of proposed actions under the new operational objectives, as well as measurable indicators to monitor the implementation of these new operational objectives. _____ 1. *[1]* Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240 (OJ L 166, 11.5.2021, p. 1).	**('DEP')**~~DEP~~, which– aims at guaranteeing the resilience, integrity and trustworthiness of the Digital Single Market, at strengthening capacities to monitor cyber-attacks and threats and to respond to them, and at reinforcing cross-border cooperation **and coordination** on cybersecurity. **The European Cybersecurity Alert System could play an important role in supporting Member States in anticipating and protecting against cyber threats, and the EU Cybersecurity Reserve could play an important role in supporting Member States, Union institutions, bodies and agencies, and DEP-associated third countries in responding to and mitigating the impacts of significant incidents, large-scale cybersecurity incidents, and large-scale equivalent cybersecurity incidents. Those impacts could include considerable material or non-material damage and serious public security and safety risks. In light of the specific roles that the Cybersecurity Alert System and the EU Cybersecurity Reserve could play, this Regulation should amend Regulation (EU) 2021/694 as regards the participation of legal entities that are established in the Union but are controlled from third countries, in cases where there is a real risk that the necessary and sufficient tools, infrastructures and services, or technology, expertise and capacity, will not be available in the Union and the benefits of including such entities outweigh the security risk.**~~This will be~~

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
			~~complemented by~~ The specific conditions under which financial support may be granted for **actions implementing the Cybersecurity Alert System and the EU Cybersecurity Reserve** ~~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. _____ 1. ~~Regulation~~**[1Regulation** (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).
Recital 9			
20	(9) The financing of actions under this Regulation should be provided for in Regulation (EU) 2021/694, which should remain the relevant basic act for these actions enshrined within the Specific Objective 3 of DEP. Specific conditions for participation concerning each action will be provided for in the relevant work programmes, in line with the applicable provision of Regulation (EU) 2021/694.	(9) The financing of actions under this Regulation should be provided for in Regulation (EU) 2021/694, which should remain the relevant basic act for these actions enshrined within – the Specific Objective 3 of DEP. Specific conditions for participation concerning each action will be provided for in the relevant work programmes, in line with the applicable provision of Regulation (EU) 2021/694.	(9) The financing of actions under this Regulation should be provided for in Regulation (EU) 2021/694, which should remain the relevant basic act for these actions enshrined within the Specific Objective 3 of DEP. Specific conditions for participation concerning each action will be provided for in the relevant work programmes, in line with the applicable provision of Regulation (EU) 2021/694.
Recital 9a			

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
20a		***(9a) In light of geopolitical developments and the growing cyber threat landscape (EPP 52) and in order to ensure continuity and further development of the measures laid down in this Regulation beyond 2027, particularly the European Cyber Shield and the Cybersecurity Emergency Mechanism, it is necessary to ensure a specific budget line in the multiannual financial framework for the period 2028-2034. Member States should endevour to commit themselves to supporting all necessary measures to reduce cyber threats and incidents throughout the Union and to strengthen solidarity.***	
Recital 10			
21	(10) Horizontal financial rules adopted by the European Parliament and by the Council on the basis of Article 322 TFEU apply to this Regulation. Those rules are laid down in the Financial Regulation and determine in particular the procedure for establishing and implementing the Union budget, and provide for checks on the responsibility of financial actors. Rules adopted on the basis of Article 322 TFEU also include a general regime of conditionality for the protection of the Union budget as established in Regulation (EU, Euratom) 2020/2092 of the European Parliament and of the Council.	(10) Horizontal financial rules adopted by the European Parliament and by the Council on the basis of Article 322 TFEU apply to this Regulation. Those rules are laid down in ***Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council***[1] ~~*the Financial Regulation*~~ and determine in particular the procedure for establishing and implementing the Union budget, and provide for checks on the responsibility of financial actors. Rules adopted on the basis of Article 322 TFEU also include a general regime of conditionality for the protection of the Union budget as established in Regulation (EU, Euratom) 2020/2092 of the European	(10) Horizontal financial rules adopted by the European Parliament and by the Council on the basis of Article 322 TFEU apply to this Regulation. Those rules are laid down in the Financial Regulation and determine in particular the procedure for establishing and implementing the Union budget, and provide for checks on the responsibility of financial actors. Rules adopted on the basis of Article 322 TFEU also include a general regime of conditionality for the protection of the Union budget as established in Regulation (EU, Euratom) 2020/2092 of the European Parliament and of the Council.

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
		Parliament and of the Council[2]. _____ *1. Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union, amending Regulations (EU) No 1296/2013, (EU) No 1301/2013, (EU) No 1303/2013, (EU) No 1304/2013, (EU) No 1309/2013, (EU) No 1316/2013, (EU) No 223/2014, (EU) No 283/2014, and Decision No 541/2014/EU and repealing Regulation (EU, Euratom) No 966/2012 (OJ L 193, 30.7.2018, p. 1, ELI: http://data.europa.eu/eli/reg/2018/1046/oj).* *2. Regulation (EU, Euratom) 2020/2092 of the European Parliament and of the Council of 16 December 2020 on a general regime of conditionality for the protection of the Union budget (OJ L 433I , 22.12.2020, p. 1, ELI: http://data.europa.eu/eli/reg/2020/2092/oj).*	
Recital 11			
22	(11) For the purpose of sound financial management, specific rules should be laid down for the carry-over of unused commitment and payment appropriations. While respecting the principle that the Union budget is set annually, this Regulation should, on account of the unpredictable, exceptional and specific nature of the cybersecurity landscape, provide for possibilities to carry over unused funds beyond those set out in the Financial Regulation, thus maximising the Cybersecurity Emergency Mechanism's capacity to support Member States in countering effectively cyber threats.	(11) For the purpose of sound financial management, specific rules should be laid down for the carry-over of unused commitment and payment appropriations. While respecting the principle that the Union budget is set annually, this Regulation should, on account of the unpredictable, exceptional and specific nature of the cybersecurity landscape, provide for possibilities to carry over unused funds beyond those set out in ~~*the Financial Regulation*~~*Regulation (EU, Euratom) 2018/1046*, thus maximising the Cybersecurity Emergency Mechanism's capacity to support Member States in countering effectively cyber threats.	(11) ~~For the purpose of sound financial management, specific rules should be laid down for the carry-over of unused commitment and payment appropriations. While respecting the principle that the Union budget is set annually, this Regulation should, on account of the unpredictable, exceptional and specific nature of the cybersecurity landscape, provide for possibilities to carry over unused funds beyond those set out in~~**While prevention and preparedness measures are essential to enhance the resilience of the Union in facing significant incidents, large-scale cybersecurity incidents, and large-scale-equivalent cybersecurity incidents, the**

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
			occurrence, timing and magnitude of such incidents are by their nature unpredictable. The financial resources required to ensure an adequate response can vary significantly from year to year and should be capable of being made available immediately. Reconciling the budgetary principle of predictability with the necessity to react rapidly to new needs therefore requires adaptation of the financial ~~Regulation, thus maximising~~**implementation of the work programmes. Consequently, it is appropriate to authorise carry-over of unused appropriations, limited to the following year and solely to** the Cybersecurity Emergency Mechanism~~'s capacity to support Member States in countering effectively cyber threats~~**, in addition to the carry-over of appropriations authorised under Article 12(4) of the Financial Regulation**.
Recital 11a			
22a		***(11a) The Cybersecurity Emergency Mechanism and the EU Cybersecurity Reserve established in this Regulation are new initiatives and were not envisaged in the establishment of the multiannual financial framework for 2021-2027, and funding for those initiatives is intended to limit the reduction of funding for other priorities in the Digital Europe Programme to the minimum extent possible. The amount of the financial***	

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
		resources dedicated to the EU Cyber Security Reserve should therefore be decreased and it should be primarily drawn from the unallocated margins under the multiannual financial framework ceilings or mobilised through the non-thematic multiannual financial framework special instruments. Any earmarking or reallocation of funds from existing programmes should be kept to an absolute minimum, in order to shield existing programmes, in particular Erasmus+, from negative impact and ensure that those programmes can achieve their set objectives.	
Recital 12			
23	(12) To more effectively prevent, assess and respond to cyber threats and incidents, it is necessary to develop more comprehensive knowledge about the threats to critical assets and infrastructures on the territory of the Union, including their geographical distribution, interconnection and potential effects in case of cyber-attacks affecting those infrastructures. A large-scale Union infrastructure of SOCs should be deployed ('the European Cyber Shield'), comprising of several interoperating cross-border platforms, each grouping together several National SOCs. That infrastructure should serve national and Union cybersecurity interests and needs, leveraging state of the art technology for advanced data collection and analytics tools, enhancing cyber detection and	(12) To more effectively prevent, assess,***respond to, and recover from,*** ~~***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***~~ ***proactive approach to identifying, mitigating, and preventing potential cyber threats includes an increased capacity of advanced detection capabilities necessary to stop advanced persistent threats. Threat intelligence is information collected, analysed, and interpreted to understand potential threats and***	(12) To more effectively prevent, assess and respond to cyber threats and incidents, it is necessary to develop more comprehensive knowledge about the threats to critical assets and infrastructures on the territory of the Union, including their geographical distribution, interconnection and potential effects in case of cyber-attacks affecting those infrastructures. ~~A large-scale Union infrastructure of SOCs should be deployed (~~'The European ~~Cyber Shield'), comprising~~**Cybersecurity Alert System consists** of several interoperating cross-border ~~platforms~~**Cyber Hubs** , each grouping together ~~several~~ **three or more** National ~~SOCs~~**Cyber Hubs**. That infrastructure should serve national and Union cybersecurity interests and needs, leveraging ~~state of the art technology~~

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
	management capabilities and providing real-time situational awareness. That infrastructure should serve to increase detection of cybersecurity threats and incidents and thus complement and support Union entities and networks responsible for crisis management in the Union, notably the EU Cyber Crises Liaison Organisation Network ('EU-CyCLONe'), as defined in Directive (EU) 2022/2555 of the European Parliament and of the Council[1]. 1. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80).	***risks. By analysing and correlating vast amounts of data, it uncovers patterns, trends, and indicators of compromise that can reveal malicious activities or vulnerabilities. A network of*** SOCs should be deployed ('the European Cyber Shield'), comprising of several interoperating cross-border platforms, each grouping together several National SOCs. That infrastructure should serve national and Union cybersecurity interests and needs, leveraging state of the art technology for advanced data collection and analytics tools, enhancing cyber detection and management capabilities and providing real-time situational awareness. ***A National SOC refers to a centralised capacity responsible for continuously gathering threat intelligence information and improving the cybersecurity posture of entities under national jurisdiction by preventing, detecting, and analysing cybersecurity threats.*** That infrastructure should serve to increase detection of cybersecurity threats and incidents and thus complement and support Union entities and networks responsible for crisis management in the Union, notably the EU Cyber Crises Liaison Organisation Network ('EU-CyCLONe'), as defined in Directive (EU) 2022/2555 of the European Parliament and of the Council[1]. 1. ***[1]*** Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, p.	~~for advanced data collection~~ **state-of-the-art technology for advanced collection of relevant and, where appropriate, anonymised data** and analytics tools, enhancing **coordinated** cyber detection and management capabilities and providing real-time situational awareness. That infrastructure should serve to increase detection of cybersecurity threats and incidents and thus complement and support Union entities and networks responsible for crisis management in the Union, notably the EU Cyber Crises Liaison Organisation Network ('EU-CyCLONe')~~, as defined in Directive (EU) 2022/2555 of the European Parliament and of the Council~~[1]. 1. ~~Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80).~~

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
		80).	
Recital 13			
24	(13) Each Member State should designate a public body at national level tasked with coordinating cyber threat detection activities in that Member State. These National SOCs should act as a reference point and gateway at national level for participation in the European Cyber Shield and should ensure that cyber threat information from public and private entities is shared and collected at national level in an effective and streamlined manner.	(13) ***In order to participate in the Cyber Shield,*** each Member State should designate a public body at national level tasked with coordinating cyber threat detection activities in that Member State. ***Member States are encouraged to incorporate the National SOC capacity into their existing cyber structure and governance in order to avoid creating additional governance layers and to align this Regulation with existing legislative act, including Directive (EU) 2022/2555.*** These National SOCs should act as a reference point and gateway at national level for participation ***of private and public entities, particularly their National SOCs,*** in the European Cyber Shield and should ensure that cyber threat information from public and private entities is shared and collected at national level in an effective and streamlined manner. ***National SOCs should strengthen the cooperation and information sharing between public and private entities to break up currently existing communication silos. In doing so, they may support the creation of data exchange models and should facilitate and encourage the sharing of information in a trusted and secure environment. Close and coordinated cooperation between public and private entities is central to strengthening the Union's***	(13) **Participation in the European Cybersecurity Alert System is voluntary for Member States.** Each Member State **that decides to join the European Cybersecurity Alert System** should designate a ~~public body at~~**National Cyber Hub. This** National ~~level tasked with coordinating~~**Cyber Hub could be an entity mandated under Union law for cyber security related tasks such as CSIRTs (Computer Security Incident Response Teams), a national** cyber ~~threat detection activities in that~~**crisis management authority or other competent authority designated or established under Directive 2022/2555, or another entity acting under the authority of the** Member State~~. These National SOCs should~~ **which has the capacity to** act as a reference point and gateway at national level for participation in the European **Cybersecurity Alert System** ~~Cyber Shield~~ and should**, in particular, be capable of detecting malicious events, cyber threats and incidents, through data relevant to cyber threats and incidents, including by using state-of-the-art technologies. Member States should be able to decide to designate an existing entity to conduct the functions of** ~~ensure that cyber threat information from public and private entities is shared and collected at~~ National ~~level~~

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
		resilience in the cybersecurity sphere.	~~in an effective and streamlined manner~~**Cyber Hub, or establish a new one consisting of one or more entities under the authority of a Member State. The Cybersecurity Alert System should enhance the CSIRTs network's capabilities by sharing relevant information in order to support the network and cooperate with it in conducting its activities**.
Recital 14			
25	(14) As part of the European Cyber Shield, a number of Cross-border Cybersecurity Operations Centres ('Cross-border SOCs') should be established. These should bring together National SOCs from at least three Member States, so that the benefits of cross-border threat detection and information sharing and management can be fully achieved. The general objective of Cross-border SOCs should be to strengthen capacities to analyse, prevent and detect cybersecurity threats and to support the production of high-quality intelligence on cybersecurity threats, notably through the sharing of data from various sources, public or private, as well as through the sharing and joint use of state-of-the-art tools, and jointly developing detection, analysis and prevention capabilities in a trusted environment. They should provide new additional capacity, building upon and complementing existing SOCs and computer incident response teams	(14) As part of the European Cyber Shield, a number of Cross-border Cybersecurity Operations Centres ('Cross-border SOCs') should be established. These should bring together National SOCs from at least three Member States, so that the benefits of cross-border threat detection and information sharing and management can be fully achieved. The general objective of Cross-border SOCs should be to strengthen capacities to analyse, prevent and detect cybersecurity threats and to support the production of high-quality intelligence ***including collecting and sharing data and information on possible malicious hacking, newly developed maliciuous threaths and exploits that have not yet deployed in a cyber-incidents, and analysis efforts,*** on cybersecurity threats, notably through the sharing of data from various sources, public or private, as well as through the sharing and joint use of state-of-the-art tools, and jointly	(14) As part of the European ~~Cyber Shield~~**Cybersecurity Alert System** , a number of ~~Cross-border Cybersecurity Operations Centres ('Cross-border SOCs')~~ **Cross-Border Cyber Hubs** should be established. These should bring together National ~~SOCs~~ **Cyber Hubs** from at least three Member States, so that the benefits of cross-border threat detection and information sharing and management can be fully achieved. The general objective of ~~Cross-border SOCs~~**Cross Border Cyber Hubs'** should be to strengthen capacities to analyse, prevent and detect cybersecurity threats and to support the production of high-quality intelligence on cybersecurity threats, notably through the sharing of ~~data~~ **relevant and, where appropriate, anonymised information** 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

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
	(‘CSIRTs’) and other relevant actors.	developing detection, analysis and prevention capabilities in a trusted ***and secure*** environment ***with the support of ENISA, in matters related to operational cooperation among Member States. Cross-border SOCs***. ~~*They*~~ should ***facilitate and encourage the sharing of information in a trusted and secure environment andshould*** provide new additional capacity, building upon and complementing existing SOCs and computer incident response teams (‘CSIRTs’) and other relevant actors.	environment. They should provide new additional capacity, building upon and complementing existing SOCs and ~~computer incident response teams (~~ ‘CSIRTs’~~)~~ and other relevant actors**, including the CSIRTs network**.
Recital 14a			
25a			**(14a) A Member State selected by the European Cybersecurity Competence Centre (‘ECCC’) following a call for expression of interest to set up a National Cyber Hub or enhance the capabilities of an existing one, should purchase relevant tools, infrastructures and services jointly with the ECCC. Such a Member State should be eligible to receive a grant to operate the tools, infrastructures and services. A Hosting Consortium consisting of at least three Member States, which has been selected by the ECCC following a call for expression of interest to set up a Cross-Border Cyber Hub or enhance the capabilities of an existing one, should purchase relevant tools, infrastructures and services jointly with the ECCC. Such a Hosting Consortium should be eligible to receive a grant to operate the**

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
			tools, infrastructures and services. The procurement procedure to purchase the relevant tools, infrastructures and services should be carried out jointly by the ECCC and relevant contracting authorities from the Member States selected following these calls for expressions of interest. **This procurement should be in accordance with Article 165(2) of Regulation EU 2018/1046, and Article 90 of Decision no GB/2023/1 of the Governing Board of the ECCC. Private entities should therefore not be eligible to participate in the calls for expression of interest to jointly purchase tools, infrastructures and services with the ECCC, or to receive grants to operate those tools, infrastructures and services.** **However, the Member States should have the possibility to involve private entities in the setting up, enhancement and operation of their National Cyber Hubs and Cross Border Cyber Hub in other ways which they deem appropriate, in compliance with national and Union law. Private entities could also be eligible to receive Union funding in accordance with Regulation (EU) 2021/887 in order to provide support to National Cyber Hubs.**
Recital 14b			
25b			**(14b) In order to enhance cyber threat detection and situational awareness in the**

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
			Union, a Member State which is selected following a call for expression of interest to set up a National Cyber Hub or enhance the capabilities of an existing one, should commit to apply to participate in a Cross-Border Cyber Hub. If a Member State is not a participant in a Cross-border Cyber Hub within two years from the date on which the tools, infrastructures and services are acquired, or on which it receives grant funding, whichever occurs sooner, it should not be eligible to participate in further Union support actions to enhance the capabilities of its National Cyber Hub provided for in Chapter II of this Regulation. In such cases entities from Member States could still participate in calls for proposals on other topics under DEP or other European funding programs, including calls on capacities for cyber detection and information sharing, provided that those entities meet the eligibility criteria established in the programs.
Recital 15			
26	(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-	(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-	(15) ~~At national level, the monitoring, detection and analysis of cyber threats is typically ensured by SOCs of public and private entities, in combination with CSIRTs. In addition,~~**CSIRTs exchange information in the context of the CSIRT network, in accordance with Directive (EU) 2022/2555. The EU**

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
	border SOCs should constitute a new capability that is complementary to the CSIRTs network, by pooling and sharing data on cybersecurity threats from public and private entities, enhancing the value of such data through expert analysis and jointly acquired infrastructures and state of the art tools, and contributing to the development of Union capabilities and technological sovereignty.	border SOCs should constitute a new ~~capability~~***capacity*** that is ~~complementary to the~~ ***incorporated into the existing cybersecurity infrastructure, particularly*** CSIRTs network, by pooling and sharing data on cybersecurity threats from public and private entities, ***in particular their SOCs,*** enhancing the value of such data through expert analysis and jointly acquired infrastructures and state of the art tools, and contributing to the ***Union's technological sovereignty, its open strategic autonomy, competitiveness and resilience and to the*** development of ~~Union capabilities and technological sovereignty~~***a significant cybersecurity ecosystem, including in cooperation with trusted and like-minded international partners***.	**Cybersecurity Alert System should constitute a new capability that is complementary to the** CSIRTs ~~exchange information in the context of the CSIRT network, in accordance with Directive (EU) 2022/2555. The Cross-border SOCs should constitute a new capability that is complementary to~~**network by contributing to building a Union situational awareness allowing the reinforcement of the capabilities of the latter. Cross Border Cyber Hubs should coordinate and cooperate closely with** the CSIRTs Network**. They should act**, by pooling **data** and sharing ~~data~~ **relevant and, where appropriate, anonymised information** 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~~**state-of-the-art** tools, and contributing to the development of Union capabilities and technological sovereignty.
Recital 16			
27	(16) The Cross-border SOCs should act as a central point allowing for a broad pooling of relevant data and cyber threat intelligence, enable the spreading of threat information among a large and diverse set of actors (e.g., Computer Emergency Response Teams ('CERTs'), CSIRTs, Information Sharing and Analysis Centers ('ISACs'), operators of critical	(16) The Cross-border SOCs should act as a central point allowing for a broad pooling of relevant data and cyber threat intelligence, enable the spreading of threat information among a large and diverse set of actors (e.g., Computer Emergency Response Teams ('CERTs'), CSIRTs, Information Sharing and Analysis Centers ('ISACs'), operators of critical	(16) The ~~Cross-border SOCs~~**Cross-Border Cyber Hub** should act as a central point allowing for a broad pooling of relevant data and cyber threat intelligence, enable the spreading of threat information among a large and diverse set of ~~actors (e.g.,~~**stakeholders (such as** Computer Emergency Response Teams ('CERTs'), CSIRTs, Information Sharing and

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
	infrastructures). The information exchanged among participants in a Cross-border SOC could include data from networks and sensors, threat intelligence feeds, indicators of compromise, and contextualised information about incidents, threats and vulnerabilities. In addition, Cross-border SOCs should also enter into cooperation agreements with other Cross-border SOCs.	infrastructures) ***with a view to facilitating the break-up of currently existing communication siloes. In doing so, Cross-border SOCs could also support the creation of data exchange models across the Union***. The information exchanged among participants in a Cross-border SOC could include data from networks and sensors, threat intelligence feeds, indicators of compromise, and contextualised information about incidents, threats and vulnerabilities ***including collecting and sharing data and information on possible malicious hacking, newly developed maliciuous threaths and exploits that have not yet deployed in a cyber-incidents, and analysis efforts***. In addition, Cross-border SOCs should also enter into cooperation agreements with other Cross-border SOCs.	Analysis Centers ('ISACs'), operators of critical infrastructures). **Members of the Hosting Consortium should specify in the consortium agreement the relevant information to be shared among the participants of the Cross-Border Cyber Hub.** The information exchanged among participants in a Cross-border ~~SOC~~**Cyber Hub** could include **for instance** data from networks and sensors, threat intelligence feeds, indicators of compromise, and contextualised information about incidents, threats**, vulnerabilities and near misses, techniques and procedures, adversarial tactics, threat actors specific information, cybersecurity alerts and recommendations regarding the configuration of cybersecurity tools to detect cyberattacks** ~~and vulnerabilities~~. In addition, ~~Cross-border SOCs~~**Cross-Border Cyber Hubs** should also enter into cooperation agreements with other ~~Cross-border SOCs~~**Cross-Border Cyber Hubs**.
Recital 16a			
27a			**(16a) The Cross-Border Cyber Hubs and the CSIRTs network should cooperate closely to ensure synergies and complementarity of activities. For that purpose, they should agree on procedural arrangements on cooperation and sharing of relevant information. This could include sharing of relevant information on cyber threats, significant cybersecurity incidents and**

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
			ensuring that experiences with state-of-the-art tools, notably Artificial Intelligence and data analytics technology, used within the Cross-Border Cyber Hubs is shared with the CSIRTs network.
Recital 17			
28	(17) Shared situational awareness among relevant authorities is an indispensable prerequisite for Union-wide preparedness and coordination with regards to significant and large-scale cybersecurity incidents. Directive (EU) 2022/2555 establishes the EU–CyCLONe to support the coordinated management of large-scale cybersecurity incidents and crises at operational level and to ensure the regular exchange of relevant information among Member States and Union institutions, bodies and agencies. Recommendation (EU) 2017/1584 on coordinated response to large-scale cybersecurity incidents and crises addresses the role of all relevant actors. Directive (EU) 2022/2555 also recalls the Commission's responsibilities in the Union Civil Protection Mechanism ('UCPM') established by Decision 1313/2013/EU of the European Parliament and of the Council, as well as for providing analytical reports for the Integrated Political Crisis Response Mechanism ('IPCR') arrangements under Implementing Decision (EU) 2018/1993. Therefore, in situations where Cross-border SOCs obtain	(17) Shared situational awareness among relevant authorities is an indispensable prerequisite for Union-wide preparedness and coordination with regards to significant and large-scale cybersecurity incidents. Directive (EU) 2022/2555 establishes the EU–CyCLONe to support the coordinated management of large-scale cybersecurity incidents and crises at operational level and to ensure the regular exchange of relevant information among Member States and Union institutions, bodies and agencies. Recommendation (EU) 2017/1584 on coordinated response to large-scale cybersecurity incidents and crises addresses the role of all relevant actors. Directive (EU) 2022/2555 also recalls the Commission's responsibilities in the Union Civil Protection Mechanism ('UCPM') established by Decision 1313/2013/EU of the European Parliament and of the Council[1], as well as for providing analytical reports for the Integrated Political Crisis Response Mechanism ('IPCR') arrangements under ***Council*** Implementing Decision (EU) 2018/1993[2]. Therefore, in situations where Cross-border	(17) Shared situational awareness among relevant authorities is an indispensable prerequisite for Union-wide preparedness and coordination with regards to significant and large-scale cybersecurity incidents. Directive (EU) 2022/2555 establishes the EU–CyCLONe to support the coordinated management of large-scale cybersecurity incidents and crises at operational level and to ensure the regular exchange of relevant information among Member States and Union institutions, bodies and agencies. ~~Recommendation (EU) 2017/1584 on coordinated response to large-scale cybersecurity incidents and crises addresses the role of all relevant actors.~~ Directive (EU) 2022/2555 also ~~recalls the Commission's responsibilities in the Union Civil Protection Mechanism ('UCPM') established by Decision 1313/2013/EU of the European Parliament and of the Council, as well as for providing analytical reports for the Integrated Political Crisis Response Mechanism ('IPCR') arrangements under Implementing Decision (EU) 2018/1993. Therefore~~**establishes the CSIRTs network to promote swift and**

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
	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.	SOCs obtain information related to a potential or ongoing large-scale cybersecurity incident, they should provide relevant information to EU-CyCLONe, the CSIRTs network and the Commission ***in accordance with Directive (EU) 2022/2555***. 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. _____ ***1. Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism Text with EEA relevance (OJ L 347, 20.12.2013, p. 924, ELI: http://data.europa.eu/eli/dec/2013/1313/oj).*** ***2. Council Implementing Decision (EU) 2018/1993 of 11 December 2018 on the EU Integrated Political Crisis Response Arrangements (OJ L 320, 17.12.2018, p. 28, ELI: http://data.europa.eu/eli/dec_impl/2018/1993/oj).***	**effective operational cooperation among all Member States. To ensure situational awareness and strengthen solidarity**, in situations where ~~Cross-border SOCs~~**Cross-Border Cyber Hubs** 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~~**inform, as an early warning, EU-CyCLONe.** . 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.
Recital 18			
29	(18) Entities participating in the European Cyber Shield should ensure a high-level of interoperability among themselves including, as appropriate, as regards data formats, taxonomy, data handling and data analysis tools, and secure communications channels, a minimum	(18) Entities participating in the European Cyber Shield should ensure a high-level of interoperability among themselves including, as appropriate, as regards data formats, taxonomy, data handling and data analysis tools, and secure communications channels, a minimum	(18) Entities participating in the European ~~Cyber Shield~~ **Cybersecurity Alert System** 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

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
	level of application layer security, situational awareness dashboard, and indicators. The adoption of a common taxonomy and the development of a template for situational reports to describe the technical cause and impacts of cybersecurity incidents should take into account the ongoing work on incident notification in the context of the implementation of Directive (EU) 2022/2555.	level of application layer security, situational awareness dashboard, and indicators. The adoption of a common taxonomy and the development of a template for situational reports to describe the technical cause and impacts of cybersecurity incidents should take into account the ongoing work on incident notification in the context of the implementation of Directive (EU) 2022/2555.	communications channels, a minimum level of application layer security, situational awareness dashboard, and indicators. The adoption of a common taxonomy and the development of a template for situational reports to describe the ~~technical cause and impacts of~~**causes of detected cyber threats and** cybersecurity ~~incidents~~**risks,** should take into account ~~the ongoing work on incident notification~~ **existing work done** in the context of the implementation of Directive (EU) 2022/2555.
Recital 19			
30	(19) In order to enable the exchange of data on cybersecurity threats from various sources, on a large-scale basis, in a trusted environment, entities participating in the European Cyber Shield should be equipped with state-of-the-art and highly-secure tools, equipment and infrastructures. This should make it possible to improve collective detection capacities and timely warnings to authorities and relevant entities, notably by using the latest artificial intelligence and data analytics technologies.	(19) In order to enable the exchange of data on cybersecurity threats from various sources, on a large-scale basis, in a trusted ***and secure*** environment, entities participating in the European Cyber Shield should be equipped with state-of-the-art and highly-secure tools, equipment and infrastructures ***and skilled personnel***. 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.	(19) In order to enable the exchange of ~~data~~ **information** on cybersecurity threats from various sources, on a large-scale basis, in a trusted environment, entities participating in the European ~~Cyber Shield~~ **Cybersecurity Alert System** should be equipped with state-of-the-art and highly-secure tools, equipment and infrastructures**. The Commission, after consulting the CSIRTs Network, EU-CyCLONe, the NIS Cooperation Group and ENISA, should be able to issue guidance in this respect, with due respect to national defence and security interests**. This should make it possible to improve collective detection capacities and timely warnings to authorities and relevant entities, notably by using the latest artificial intelligence and data analytics technologies.

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
Recital 20			
31	(20) By collecting, sharing and exchanging data, the European Cyber Shield should enhance the Union's technological sovereignty. The pooling of high-quality curated data should also contribute to the development of advanced artificial intelligence and data analytics technologies. It should be facilitated through the connection of the European Cyber Shield with the pan-European High Performance Computing infrastructure established by Council Regulation (EU) 2021/1173[1]. _____ 1. Council Regulation (EU) 2021/1173 of 13 July 2021 on establishing the European High Performance Computing Joint Undertaking and repealing Regulation (EU) 2018/1488 (OJ L 256, 19.7.2021, p. 3).	(20) By collecting, sharing and exchanging data, the European Cyber Shield should enhance the Union's technological sovereignty, ***its open strategic autonomy, competitiveness and resilience and an EU significant cybersecurity ecosystem***. The pooling of high-quality curated data should also contribute to the development of advanced artificial intelligence and data analytics technologies. ***Artificial intelligence is the most effective when paired with human analysis. Therefore, a skilled labour force remains essential for pooling high-quality data.*** It should be facilitated through the connection of the European Cyber Shield with the pan-European High Performance Computing infrastructure established by Council Regulation (EU) 2021/1173[1]. _____ 1. ***[1]*** Council Regulation (EU) 2021/1173 of 13 July 2021 on establishing the European High Performance Computing Joint Undertaking and repealing Regulation (EU) 2018/1488 (OJ L 256, 19.7.2021, p. ~~3)~~ ***3, ELI: http://data.europa.eu/eli/reg/2021/1173/oj)***.	(20) By collecting, **analysing,** sharing and exchanging **relevant data and information** ~~data~~, the European **Cybersecurity Alert System** ~~Cyber Shield~~ should enhance the Union's technological sovereignty. The pooling of high-quality curated data ~~should~~ **could** also contribute to the development of advanced artificial intelligence and data analytics technologies. ~~It should be facilitated through the connection of the European Cyber Shield with the pan-European High Performance Computing infrastructure established by Council Regulation (EU) 2021/1173[1].~~ _____ ~~1. Council Regulation (EU) 2021/1173 of 13 July 2021 on establishing the European High Performance Computing Joint Undertaking and repealing Regulation (EU) 2018/1488 (OJ L 256, 19.7.2021, p. 3).~~
Recital 21			
32	(21) While the European Cyber Shield is a civilian project, the cyber defence community could benefit from stronger civilian detection and situational awareness capabilities developed	(21) While the European Cyber Shield is a civilian project, the cyber defence community could benefit from stronger civilian detection and situational awareness capabilities developed	(21) While the European ~~Cyber Shield~~ **Cybersecurity Alert System** is a civilian project, the cyber defence community could benefit from stronger civilian detection and

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
	for the protection of critical infrastructure. Cross-border SOCs, with the support of the Commission and the European Cybersecurity Competence Centre ('ECCC'), and in cooperation with the High Representative of the Union for Foreign Affairs and Security Policy (the 'High Representative'), should gradually develop dedicated protocols and standards to allow for cooperation with the cyber defence community, including vetting and security conditions. The development of the European Cyber Shield should be accompanied by a reflection enabling future collaboration with networks and platforms responsible for information sharing in the cyber defence community, in close cooperation with the High Representative.	for the protection of critical infrastructure. Cross-border SOCs, with the support of the Commission and the European Cybersecurity Competence Centre ('ECCC'), and in cooperation with the High Representative of the Union for Foreign Affairs and Security Policy (the 'High Representative'), should gradually develop dedicated ***access conditions and safeguards*** protocols and standards to allow for cooperation with the cyber defence community, including vetting and security conditions, ***respecting the civilian character of institutions and the destination of funding, therefore using the funds available to the defence community.***. The development of the European Cyber Shield should be accompanied by a reflection enabling future collaboration with networks and platforms responsible for information sharing in the cyber defence community, in close cooperation with the High Representative ***and in full respect of rights and freedoms***..	situational awareness capabilities developed for the protection of critical infrastructure. ~~Cross-border SOCs, with the support of the Commission and the European Cybersecurity Competence Centre ('ECCC'), and in cooperation with the High Representative of the Union for Foreign Affairs and Security Policy (the 'High Representative'), should gradually develop dedicated protocols and standards to allow for cooperation with the cyber defence community, including vetting and security conditions. The development of the European Cyber Shield should be accompanied by a reflection enabling future collaboration with networks and platforms responsible for information sharing in the cyber defence community, in close cooperation with the High Representative.~~
Recital 22			
33	(22) Information sharing among participants of the European Cyber Shield should comply with existing legal requirements and in particular Union and national data protection law, as well as the Union rules on competition governing the exchange of information. The recipient of the information should implement, insofar as the processing of personal data is necessary, technical and organisational measures that	(22) Information sharing among participants of the European Cyber Shield should comply with existing legal requirements and in particular Union and national data protection law, as well as the Union rules on competition governing the exchange of information. The recipient of the information should implement, insofar as the processing of personal data is necessary, technical and organisational measures that	(22) Information sharing among participants of the European ~~Cyber Shield~~ **Cybersecurity Alert System** 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,

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
	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.	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.	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.
Recital 22a			
33a			**(22a) Information sharing under this Regulation could take place using non-disclosure agreements, or informal guidance on information distribution such as the traffic light protocol. The Traffic Light Protocol (TLP) is to be understood as a means to provide information about any limitations with regard to the further spreading of information. It is used in almost all CSIRTs and in some information analysis and sharing centers.**
Recital 23			
34	(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	(23) Without prejudice to Article 346 of TFEU, the exchange of information that is confidential pursuant to Union or national ~~*rules*~~***law*** 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	(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~~

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
	of trade and business secrets.	of trade and business secrets.	~~of trade and business secrets.~~
Recital 24			
35	(24) In view of the increasing risks and number of cyber incidents affecting Member States, it is necessary to set up a crisis support instrument to improve the Union's resilience to significant and large-scale cybersecurity incidents and complement Member States' actions through emergency financial support for preparedness, response and immediate recovery of essential services. That instrument should enable the rapid deployment of assistance in defined circumstances and under clear conditions and allow for a careful monitoring and evaluation of how resources have been used. Whilst the primary responsibility for preventing, preparing for and responding to cybersecurity incidents and crises lies with the Member States, the Cyber Emergency Mechanism promotes solidarity between Member States in accordance with Article 3(3) of the Treaty on European Union ('TEU').	(24) In view of the increasing risks and number of cyber incidents affecting Member States, it is necessary to set up a crisis support instrument to improve the Union's resilience to significant and large-scale cybersecurity incidents and complement Member States' actions through emergency financial support for preparedness, response and immediate recovery of essential services. That instrument should enable the rapid ***and effective*** 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*~~***Cybersecurity*** Emergency Mechanism promotes solidarity between Member States in accordance with Article 3(3) of the Treaty on European Union ('TEU').	(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**, large-scale and large-scale-equivalent** ~~and large-scale~~ cybersecurity incidents and complement Member States' actions through emergency financial support for preparedness, response and ~~immediate~~ **initial** recovery of essential services**. As the full recovery from an incident is a comprehensive process of restoring functioning of the entity affected by the incident to the state from before the incident and could be a long process that entails significant costs, the support from the EU Cybersecurity Reserve should be limited to the initial stage of the recovery process, leading to the restoration of basic functionalities of the systems**. That instrument should enable the rapid deployment of assistance in defined circumstances and under clear conditions and allow for a careful monitoring and evaluation of how resources have been used. Whilst the primary responsibility for preventing, preparing for and responding to cybersecurity incidents and crises lies with the Member States, the Cyber Emergency Mechanism promotes solidarity

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
			between Member States in accordance with Article 3(3) of the Treaty on European Union ('TEU').
Recital 25			
36	(25) The Cyber Emergency Mechanism should provide support to Member States complementing their own measures and resources, and other existing support options in case of response to and immediate recovery from significant and large-scale cybersecurity incidents, such as the services provided by the European Union Agency for Cybersecurity ('ENISA') in accordance with its mandate, the coordinated response and the assistance from the CSIRTs network, the mitigation support from the EU-CyCLONe, as well as mutual assistance between Member States including in the context of Article 42(7) of TEU, the PESCO Cyber Rapid Response Teams[1] and Hybrid Rapid Response Teams. It should address the need to ensure that specialised means are available to support preparedness and response to cybersecurity incidents across the Union and in third countries. _____ 1. COUNCIL DECISION (CFSP) 2017/ 2315 - of 11 December 2017 - establishing permanent structured cooperation (PESCO) and determining the list of participating Member States.	(25) The ~~Cyber~~***Cybersecurity*** Emergency Mechanism should provide support to Member States complementing their own measures and resources,~~–~~ and other existing support options in case of response to and immediate recovery from significant and large-scale cybersecurity incidents, such as the services provided by the European Union Agency for Cybersecurity ('ENISA') in accordance with its mandate, the coordinated response and the assistance from the CSIRTs network, the mitigation support from the EU-CyCLONe, as well as mutual assistance between Member States including in the context of Article 42(7) of TEU, the PESCO Cyber Rapid Response Teams[1] and Hybrid Rapid Response Teams. It should address the need to ensure that specialised means are available to support preparedness and response to cybersecurity incidents across the Union and in third countries. _____ 1. ***[1]*** COUNCIL DECISION (CFSP) 2017/ 2315 - of 11 December 2017 - establishing permanent structured cooperation (PESCO) and determining the list of participating Member States.	(25) The Cyber Emergency Mechanism should provide support to Member States complementing their own measures and resources,~~–~~ and other existing support options in case of response to and~~ immediate~~ **initial** recovery from significant and large-scale cybersecurity incidents, such as the services provided by the European Union Agency for Cybersecurity ('ENISA') in accordance with its mandate, the coordinated response and the assistance from the CSIRTs network, the mitigation support from the EU-CyCLONe, as well as mutual assistance between Member States including in the context of Article 42(7) of TEU, the PESCO Cyber Rapid Response Teams[1] ~~and Hybrid Rapid Response Teams~~. It should address the need to ensure that specialised means are available to support preparedness**, response and recovery**~~ and response~~ to cybersecurity incidents across the Union and in **DEP-associated** third countries. _____ 1. COUNCIL DECISION (CFSP) 2017/ 2315 - of 11 December 2017 - establishing permanent structured cooperation (PESCO) and determining the list of participating Member States.

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
Recital 26			
37	(26) This instrument is without prejudice to procedures and frameworks to coordinate crisis response at Union level, in particular the UCPM[1], IPCR[2,] and Directive (EU) 2022/2555. It may contribute to or complement actions implemented in the context of Article 42(7) of TEU or in situations defined in Article 222 of TFEU. The use of this instrument should also be coordinated with the implementation of Cyber Diplomacy Toolbox's measures, where appropriate. _____ 1. Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism (OJ L 347, 20.12.2013, p. 924). 2. Integrated Political Crisis Response arrangements (IPCR) and in accordance with Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises.	(26) This instrument is without prejudice to procedures and frameworks to coordinate crisis response at Union level, in particular the UCPM[1], IPCR[2,] and Directive (EU) 2022/2555. It may contribute to or complement actions implemented in the context of Article 42(7) of TEU or in situations defined in Article 222 of TFEU. The use of this instrument should also be coordinated with the implementation of Cyber Diplomacy Toolbox's measures, where appropriate. _____ 1. Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism (OJ L 347, 20.12.2013, p. 924). 2. Integrated Political Crisis Response arrangements (IPCR) and in accordance with Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises.	(26) This ~~instrument~~ **Regulation** is without prejudice to procedures and frameworks to coordinate crisis response at Union level, in particular the ~~UCPM[1], IPCR[2,]~~**Union Civil Protection Mechanism established under Decision No 1313/2013/EU of the European Parliament and of the Council[1], the EU Integrated Political Crisis Response Arrangements under Council Implementing Decision (EU) 2018/1993 [2] (IPCR Arrangements), Commission Recommendation 2017/1584[3]** and Directive (EU) 2022/2555. ~~It may contribute to or~~**Support provided under the Cyber Emergency Mechanism can complement assistance provided in the context of the Common Foreign and Security Policy and the Common Security and Defence Policy, including through the Cyber Rapid Response Teams, taking into account the civilian nature of the Mechanism. Support provided under the Cyber Emergency Mechanism can** 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** ~~or~~ in situations **referred to** ~~defined~~ in Article 222 ~~of TFEU. The use~~ **TFEU. The implementation** of this ~~instrument~~**Regulation** should also be coordinated with the

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
			implementation of **measures under the** Cyber Diplomacy Toolbox[2]~~'s measures~~, where appropriate. _____ 1. Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism (OJ L 347, 20.12.2013, p. 924). 2. ~~Integrated Political Crisis Response arrangements (IPCR~~**Council Implementing Decision (EU)** ~~and in accordance with Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated~~**2018/1993 of 11 December 2018 on the EU Integrated Political Crisis** Response ~~to large-scale cybersecurity incidents and crises~~**Arrangements (OJ L 320, 17.12.2018, p. 28)**. **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).**
Recital 27			
38	(27) Assistance provided under this Regulation should be in support of, and complementary to, the actions taken by Member States at national level. To this end, close cooperation and consultation between the Commission and the affected Member State should be ensured. When requesting support under the Cyber Emergency Mechanism, the Member State should provide relevant information justifying the need for support.	(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***, ENISA*** and the affected Member State should be ensured. When requesting support under the ~~*Cyber*~~***Cybersecurity*** Emergency Mechanism, the Member State should provide relevant information justifying the need for support.	(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 **Member States and** the Commission and**, where relevant, ENISA and the ECCC,** ~~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.
Recital 28			

www.parlament.gv.at

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

www.parlament.gv.at

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

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
	in coordination with relevant civilian and military bodies and agencies and established networks, including the EU CyCLONe, as well as the risk assessment of communications networks and infrastructures requested by the Joint Ministerial Call of Nevers and conducted by the NIS Cooperation Group, with the support of the Commission and ENISA, and in cooperation with the Body of European Regulators for Electronic Communications (BEREC), the coordinated risk assessments to be conducted under Article 22 of Directive (EU) 2022/2555 and digital operational resilience testing as provided for in Regulation (EU) 2022/2554 of the European Parliament and of the Council[1]. The selection of sectors should also take into account the Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure. _____ 1. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011	with relevant civilian and military bodies and agencies and established networks, including the ~~*EU CyCLONe*~~***EU-CyCLONe***, as well as the risk assessment of communications networks and infrastructures requested by the Joint Ministerial Call of Nevers and conducted by the NIS Cooperation Group, with the support of the Commission and ENISA, and in cooperation with the Body of European Regulators for Electronic Communications (BEREC), the coordinated risk assessments to be conducted under Article 22 of Directive (EU) 2022/2555 and digital operational resilience testing as provided for in Regulation (EU) 2022/2554 of the European Parliament and of the Council[1]. The selection of sectors should also take into account the Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure. _____ 1. ***[1]*** Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011	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~~**EU-CyCLONe**, as well as the risk assessment of communications networks and infrastructures requested by the Joint Ministerial Call of Nevers and conducted by the NIS Cooperation Group, with the support of the Commission and ENISA, and in cooperation with the Body of European Regulators for Electronic Communications (BEREC), the coordinated risk assessments to be conducted under Article 22 of Directive (EU) 2022/2555 and digital operational resilience testing as provided for in Regulation (EU) 2022/2554 of the European Parliament and of the Council[1]. The selection of sectors should also take into account the Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure. _____ 1. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011
Recital 30			
41	(30) In addition, the Cyber Emergency	(30) In addition, the ~~*Cyber*~~***Cybersecurity***	(30) In addition, the Cyber Emergency

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
	Mechanism should offer support for other preparedness actions and support preparedness in other sectors, not covered by the coordinated testing of entities operating in highly critical sectors. Those actions could include various types of national preparedness activities.	Emergency Mechanism should offer support for other preparedness actions and support preparedness in other sectors, not covered by the coordinated testing of entities operating in highly critical sectors. Those actions could include various types of national preparedness activities.	Mechanism should offer support for other preparedness actions and support preparedness in other sectors, not covered by the coordinated testing of entities operating in **sectors of high criticality and other** ~~highly~~ critical sectors. Those actions could include various types of national preparedness activities.
Recital 31			
42	(31) The Cyber Emergency Mechanism should also provide support for incident response actions to mitigate the impact of significant and large-scale cybersecurity incidents, to support immediate recovery or restore the functioning of essential services. Where appropriate, it should complement the UCPM to ensure a comprehensive approach to respond to the impacts of cyber incidents on citizens.	(31) The ~~Cyber~~***Cybersecurity*** Emergency Mechanism should also provide support for incident response actions to mitigate the impact of significant and large-scale cybersecurity incidents, to support immediate recovery or restore the functioning of essential services. Where appropriate, it should complement the UCPM to ensure a comprehensive approach to respond to the impacts of cyber incidents on citizens.	(31) The Cyber Emergency Mechanism should also provide support for incident response actions to mitigate the impact of significant and large-scale cybersecurity incidents, to support ~~immediate~~**initial** recovery or restore the functioning of essential services. Where appropriate, it should complement the UCPM to ensure a comprehensive approach to respond to the impacts of cyber incidents on citizens.
Recital 32			
43	(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	(32) The ~~Cyber~~***Cybersecurity*** 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	(32) The Cyber Emergency Mechanism should support **technical** assistance provided by **a** Member ~~States to a~~ **State to another** Member State affected by a significant or large-scale cybersecurity incident, including by ~~the~~ CSIRTs ~~network set out~~ **as referred to** in Article ~~15~~ **11(3) point (f)** of Directive (EU) 2022/2555. Member States providing **such** assistance should be allowed to submit requests to cover

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
	mutual assistance. The eligible costs could include travel, accommodation and daily allowance expenses of cybersecurity experts.	framework of mutual assistance. The eligible costs could include travel, accommodation and daily allowance expenses of cybersecurity experts.	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.
Recital 32a			
43a			**(32a) Given the essential role that private companies play in the detection, preparedness and response to large-scale cybersecurity incidents, a framework for voluntary pro-bono cooperation could be established at EU level, consisting of providers willing to offer services without remuneration in cases of large-scale and large-scale equivalent cybersecurity incidents and crises. Such framework could be established by ENISA in cooperation with the EU-CyCLONe and should be compliant with the criteria applicable to trusted providers under this regulation including in relation to the trustworthiness of companies, their experience as well as the ability to handle sensitive information in a secure manner.**
Recital 33			
44	(33) A Union-level Cybersecurity Reserve should gradually be set up, consisting of services from private providers of managed	(33) A Union-level Cybersecurity Reserve should gradually be set up, consisting of services from private providers of managed	(33) **As part of the Cyber Emergency Mechanism,** a Union-level Cybersecurity Reserve should gradually be set up, consisting

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
	security services to support response and immediate recovery actions in cases of significant or large-scale cybersecurity incidents. The EU Cybersecurity Reserve should ensure the availability and readiness of services. The services from the EU Cybersecurity Reserve should serve to support national authorities in providing assistance to affected entities operating in critical or highly critical sectors as a complement to their own actions at national level. When requesting support from the EU Cybersecurity Reserve, Member States should specify the support provided to the affected entity at the national level, which should be taken into account when assessing the Member State request. The services from the EU Cybersecurity Reserve may also serve to support Union institutions, bodies and agencies, under similar conditions.	security services to support response and immediate recovery actions in cases of significant or large-scale cybersecurity incidents. The EU Cybersecurity Reserve should ensure the availability and readiness of services***, while reinforcing the Union's resilience, including the participation of European managed security services providers that are SMEs and ensuring the creation of a cybersecurity ecosystem, in particular microenterprises, SMEs including startups, with investment in research and innovation (R&I) to develop state-of-the-art technologies, such as those relating to cloud and artificial intelligence. Trusted providers, including SMEs, should be able to cooperate with one another to fulfil the criteria above.***. The services from the EU Cybersecurity Reserve should serve to support national authorities in providing assistance to affected entities operating in critical or highly critical sectors as a complement to their own actions at national level. ***Therefore, the Cybersecurity Reserve should incentivize investment in research and innovation to boost the development of these technologies. Where appropriate, common exercises with the trusted providers and potential users of the Cybersecurity Reserve could be conducted to ensure efficient functioning of the Reserve when needed.*** When requesting support from the EU Cybersecurity Reserve, Member States should specify the support provided to the affected	of services from ~~private~~ **trusted** providers ~~of managed security services~~ to support response and ~~immediate~~**initiate** recovery actions in cases of significant**, large-scale or large-scale-equivalent** ~~or large-scale~~ cybersecurity incidents **affecting Member States, Union institutions, bodies and agencies, or DEP-associated third countries**. The EU Cybersecurity Reserve should ensure the availability and readiness of services. **It should therefore include services that are committed in advance, including for instance capacities that are on stand-by and deployable at short notice. In order to ensure the effective use of Union funding, pre-committed services should be converted, in accordance with the relevant contract, into preparedness services related to incident prevention and response, in the event that those pre-committed services are not used for incident response during the time for which they are pre-committed. These services should be complementary and not duplicate the preparedness actions to be managed by the ECCC.** The services from the EU Cybersecurity Reserve should serve to support national authorities in providing assistance to affected entities operating in ~~critical or highly~~**sectors of high criticality or other** critical sectors as a complement to their own actions at national level. When requesting support from the EU Cybersecurity Reserve, ~~Member States~~ **applicants for support** should

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
		entity at the national level, which should be taken into account when assessing the Member State request. The services from the EU Cybersecurity Reserve may also serve to support Union institutions, bodies***, offices*** and agencies, under similar conditions. ***The Commission should ensure the involvement of and extensive exchanges with the Member States aiming to avoid duplication with similar initiatives, including within the North Atlantic Treaty Organization (NATO).***	specify the support provided to the affected entity at the national level, which should be taken into account when assessing the **request from the applicant. Requests for support from the EU Cybersecurity Reserve from** Member ~~State request~~**States' cyber crisis management authorities and CSIRTs, CERT-EU on behalf of the and Union institution, bodies and agencies, should be assessed by ENISA, in cases where ENISA has been entrusted with the administration and operation of the EU Cybersecurity Reserve. To facilitate the submission and assessment of requests for support, ENISA could set up a secure platform. Requests for support from DEP- associated third countries should be assessed by the Commission. EU-CyCLONe should, where relevant, be able to advise ENISA or the Commission in assessing requests for support from the EU Cybersecurity Reserve**. The services from the EU Cybersecurity Reserve may also serve to support Union institutions, bodies and agencies, under similar conditions. **It is important to take into account the European Cybersecurity Skills Framework (ECSF) when procuring the services for the reserve.**
Recital 33a			
44a			**(33a) The Commission should have overall responsibility for the functioning of the EU**

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
			Cybersecurity Reserve. Given the extensive experience gained by ENISA with the cybersecurity support action, ENISA is the most suitable Agency to implement the EU Cybersecurity Reserve, therefore the Commission should strongly consider entrusting ENISA with the operation and administration of the EU Cybersecurity Reserve. ENISA should be the contracting authority for those services with whose operation and administration it has been entrusted. ENISA should also assess requests for support from the EU Cybersecurity Reserve for such services, with the exception of requests from DEP-associated third countries where a specific procedure should apply. The procurement procedures to establish the EU Cybersecurity Reserve should be conducted in accordance with Regulation EU 2018/1046. When evaluating tenders for the purpose of establishing the EU Cybersecurity Reserve, external experts from the Member States are able to assist the evaluation committee pursuant to Article 150(3) of that Regulation. The resulting contracts, including any framework contract and specific contracts implementing a framework contract, should be signed by the contracting authority and the selected service provider. In addition, the service provider and the user to which the support under the EU Cybersecurity Reserve is provided could sign specific agreements which specify the

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
			way in which the services are to be provided and the liability conditions in case of damage caused by the services of the EU Cybersecurity Reserve. The way in which support shall be provided and the liability conditions in respect of the affected entities may be determined by national law, by the specific agreement between the service provider and the user, or by a specific agreement between the specific provider, the user and the affected entity. Appropriate agreements should be established between the parties involved clarifying roles and responsibilities and the protection of information through non-disclosure agreements. In order 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.
Recital 33b			
44b			**(33b) Member States should have a key role in the constitution, deployment and post-deployment of the EU Cybersecurity Reserve. As Regulation (EU) 2021/694 is the relevant basic act for actions implementing the EU Cybersecurity Reserve, the actions under the EU Cybersecurity Reserve should be provided for in the relevant work programmes referred to in Article 24 of Regulation (EU) 2021/694. In accordance**

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
			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, the Commission, in cooperation with EU CyCLONe, ENISA and the NIS Cooperation Group, should determine the priorities and the evolution of the EU Cybersecurity Reserve.
Recital 34			
45	(34) For the purpose of selecting private service providers to provide services in the context of the EU Cybersecurity Reserve, it is necessary to establish a set of minimum criteria that should be included in the call for tenders to select these providers, so as to ensure that the needs of Member States' authorities and entities operating in critical or highly critical sectors are met.	(34) For the purpose of selecting private service providers to provide services in the context of the EU Cybersecurity Reserve, it is necessary to establish a set of minimum criteria that should be included in the call for tenders to select these providers, so as to ensure that the needs of Member States' authorities and entities operating in critical or highly critical sectors are met. ***The participation of smaller providers, active at regional and local level should be encouraged.***	(34) For the purpose of selecting private service providers to provide services in the context of the EU Cybersecurity Reserve, it is necessary to establish a set of minimum criteria that should be included in the call for tenders to select these providers, so as to ensure that the needs of Member States' authorities and entities operating in ~~critical or highly~~**sectors of high criticality or other** critical sectors are met. **In order to address specific needs of Member States, when procuring services for the EU Cybersecurity Reserve, the contracting authority should, where appropriate, develop additional selection criteria to those laid down in this Regulation.**
Recital 35			
46			

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
	(35) To support the establishment of the EU Cybersecurity Reserve, the Commission could consider requesting ENISA to prepare a candidate certification scheme pursuant to Regulation (EU) 2019/881 for managed security services in the areas covered by the Cyber Emergency Mechanism.	(35) To support the establishment of the EU Cybersecurity Reserve, the Commission could consider requesting ENISA to prepare a candidate certification scheme pursuant to Regulation (EU) 2019/881 for managed security services in the areas covered by the ~~Cyber~~***Cybersecurity*** Emergency Mechanism. ***In order to fulfil the additional tasks deriving from this provision, ENISA should receive adequate, additional funding.***	(35) **[**To support the establishment of the EU Cybersecurity Reserve, the Commission ~~could consider requesting~~ **should request** 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.**]**
Recital 36			
47	(36) In order to support the objectives of this Regulation of promoting shared situational awareness, enhancing Union's resilience and enabling effective response to significant and large-scale cybersecurity incidents, the EU=CyCLONe, the CSIRTs network or the Commission should be able to ask ENISA to review and assess threats, vulnerabilities and mitigation actions with respect to a specific significant or large-scale cybersecurity incident. After the completion of a review and assessment of an incident, ENISA should prepare an incident review report, in collaboration with relevant stakeholders, including representatives from the private sector, Member States, the Commission and other relevant EU institutions, bodies and agencies. As regards the private sector, ENISA is developing channels for exchanging information with specialised providers,	(36) In order to support the objectives of this Regulation of promoting shared situational awareness, enhancing Union's resilience and enabling effective response to significant and large-scale cybersecurity incidents, the EU=CyCLONe, the CSIRTs network or the Commission should be able to ask ENISA to review and assess threats, vulnerabilities and mitigation actions with respect to a specific significant or large-scale cybersecurity incident. After the completion of a review and assessment of an incident, ENISA should prepare an incident review report, in collaboration with relevant stakeholders, including representatives from the private sector, Member States, the Commission and other relevant EU institutions, bodies***, offices*** and agencies. As regards the private sector, ENISA is developing channels for exchanging information with specialised providers,	(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~~**EU-CyCLONe**, **with the approval of the Member States concerned,** ~~the CSIRTs network or the Commission~~ should be able to ask ENISA to review and assess threats, **known exploitable** vulnerabilities and mitigation actions with respect to a specific significant or large-scale cybersecurity incident. After the completion of a review and assessment of an incident, ENISA should prepare an incident review report, in collaboration with **the Member State concerned,** relevant stakeholders, including representatives from the private sector, ~~Member States,~~ the Commission and other relevant EU institutions, bodies and agencies. ~~As regards the~~

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
	including providers of managed security solutions and vendors, in order to contribute to ENISA's mission of achieving a high common level of cybersecurity across the Union. Building on the collaboration with stakeholders, including the private sector, the review report on specific incidents should aim at assessing the causes, impacts and mitigations of an incident, after it has occurred. Particular attention should be paid to the input and lessons shared by the managed security service providers that fulfil the conditions of highest professional integrity, impartiality and requisite technical expertise as required by this Regulation. The report should be delivered and feed into the work of the EU=CyCLONe, the CSIRTs network and the Commission. When the incident relates to a third country, it will also be shared by the Commission with the High Representative.	including providers of managed security solutions and vendors, in order to contribute to ENISA's mission of achieving a high common level of cybersecurity across the Union. Building on the collaboration with stakeholders, including the private sector, the review report on specific incidents should aim at assessing the causes, impacts and mitigations of an incident, after it has occurred. Particular attention should be paid to the input and lessons shared by the managed security service providers that fulfil the conditions of highest professional integrity, impartiality and requisite technical expertise as required by this Regulation. The report should be delivered and feed into the work of the EU=CyCLONe, the CSIRTs network and the Commission. When the incident relates to a third country, it will also be shared by the Commission with the High Representative.	~~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~~**to EU-CyCLONe, the CSIRTs network, and the Commission and should feed into their work as well as that of ENISA**. When the incident relates to a **DEP-associated** third country, it ~~will~~ **should** also be shared by the Commission with the High Representative.
Recital 37			
48	(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	(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	(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

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
	neighbouring countries and their capacity to respond effectively to significant and large-scale cybersecurity incidents contributes to the protection of the Union as a whole. Therefore, third countries associated to the DEP may be supported from the EU Cybersecurity Reserve, where this is provided for in the respective association agreement to DEP. The funding for associated third countries should be supported by the Union in the framework of relevant partnerships and funding instruments for those countries. The support should cover services in the area of response to and immediate recovery from significant or large-scale cybersecurity incidents. The conditions set for the EU Cybersecurity Reserve and trusted providers in this Regulation should apply when providing support to the third countries associated to DEP.	neighbouring countries and their capacity to respond effectively to significant and large-scale cybersecurity incidents contributes to the protection of the Union as a whole. Therefore, third countries associated to the DEP may be supported from the EU Cybersecurity Reserve, where this is provided for in the respective association agreement to DEP. The funding for associated third countries should be supported by the Union in the framework of relevant partnerships and funding instruments for those countries. The support should cover services in the area of response to and immediate recovery from significant or large-scale cybersecurity incidents. The conditions set for the EU Cybersecurity Reserve and trusted providers in this Regulation should apply when providing support to the third countries associated to DEP.	neighbouring countries and their capacity to respond effectively to significant and large-scale cybersecurity incidents contributes to the protection of the Union**, and particularly its internal market and industry,** as a whole. ~~Therefore, third countries associated~~**Such activities could further contribute** to the ~~DEP~~ **EU cyber diplomacy. Therefore, DEP-associated third countries** may be supported from the EU Cybersecurity Reserve, **in all or part of their territories,** where this is provided for in the **agreement through which the third country is associated** ~~respective association agreement~~ to DEP. The funding for ~~associated~~**DEP-associated** third countries should be supported by the Union in the framework of relevant partnerships and funding instruments for those countries. The support should cover services in the area of response to and ~~immediate~~ **initiate** recovery from significant or large-scale cybersecurity incidents. The conditions set for the EU Cybersecurity Reserve and trusted providers in this Regulation should apply when providing support to the **DEP-associated** third countries ~~associated to DEP~~**. DEP-associated third countries should be entitled to request the service from the EU Cybersecurity Reserve when the entities targeted and for which they request support from the EU Cybersecurity Reserve, are entities operating in the sectors referred in the Annex I and II of Directive 2022/2555 and when the incidents detected**

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
			lead to an operational overrun or might have spill over effects in the Union. Support provided to DEP-associated third countries could affect the availability of the Reserve to support the Member States and Union institutions, bodies and agencies. It should be consistent with the criterion for prioritising support to Member States, Union institutions, bodies and agencies, and DEP-associated third countries. It may also affect relations with third countries, including in the context for the Common Foreign and Security Policy and Common Defence and Security Policy. Accordingly, it is appropriate that the Council reserves to itself the right to exercise implementing powers to authorise and specify the time period during which such support can be provided. Moreover, the Commission should cooperate with the High Representative in respect of such requests and support. The Commission should also take into account any view provided by ENISA in respect of the same requests and support.
Recital 37a			
48a		***(37a) Third countries could access resources and support pursuant to this Regulation, using the incident response support from the EU Cybersecurity Reserve. Furthermore, incident response service providers from third countries, including third countries associated***	

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
		to the Digital Europe Programme or other international partner countries, and NATO members, may be needed for the provision of specific services in the EU Cybersecurity Reserve. By way of derogation from Regulation (EU, Euratom) 2018/1046, in order to strengthen the Union's technological sovereignty, its open strategic autonomy, competitiveness and resilience, and to safeguard the Union's strategic assets, interests, or security, entities established in third countries that are not party to the GPA and that have not been subject to screening within the meaning of Regulation (EU) 2019/452 of the European Parliament and of the Council[1] and, where necessary, to mitigation measures, taking into account the objectives set out in this Regulation, should not be allowed to participate. The external dimension of this Regulation should be in line with the provisions established in the Association Agreement under the Digital Europe Programme. The participation of third countries should be subject to public scrutiny, with the participation of the legislative powers, to ensure that citizens can participate in the process. _____ ***1. Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union (OJ L 79I , 21.3.2019, p. 1), ELI: http://data.europa.eu/eli/reg/2019/452/oj.***	

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
Recital 37a			
48b			**(37a) Without prejudice to the rules relating to the Union's annual budget under the Treaties, the Commission should take into account the obligations arising from this Regulation when assessing the budgeting and staffing needs of ENISA.**
Recital 38			
49	(38) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission to specify the conditions for the interoperability between Cross-border SOCs; determine the procedural arrangements for the information sharing related to a potential or ongoing large-scale cybersecurity incident between Cross-border SOCs and Union entities; laying down technical requirements to ensure security of the European Cyber Shield; specify the types and the number of response services required for the EU Cybersecurity Reserve; and, specify further the detailed arrangements for allocating the EU Cybersecurity Reserve support services. Those powers should be exercised in accordance with Regulation (EU) 182/2011 of the European Parliament and of the Council.	(38) In order to ensure uniform conditions for the implementation of this Regulation,~~,~~ implementing powers should be conferred on the Commission to specify the conditions for the interoperability between Cross-border SOCs; determine the procedural arrangements for the information sharing related to a potential or ongoing large-scale cybersecurity incident between Cross-border SOCs and Union entities; laying down technical requirements to ensure security of the European Cyber Shield; specify the types and the number of response services required for the EU Cybersecurity Reserve; and, specify further the detailed arrangements for allocating the EU Cybersecurity Reserve support services. Those powers should be exercised in accordance with Regulation (EU) 182/2011 of the European Parliament and of the Council*. _____ *. ***Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011***	(38) In order to ensure uniform conditions for the implementation of this Regulation,~~,~~ implementing powers should be conferred on the Commission to~~ specify the conditions for the interoperability between Cross-border SOCs; determine the procedural arrangements for the information sharing related to a potential or ongoing large-scale cybersecurity incident between Cross-border SOCs and Union entities; laying down technical requirements to ensure security of the European Cyber Shield;~~ specify the types and the number of response services required for the EU Cybersecurity Reserve;~~ and, specify further the detailed arrangements for allocating the EU Cybersecurity Reserve support services.~~ Those powers should be exercised in accordance with Regulation (EU) 182/2011 of the European Parliament and of the Council.

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
		laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13, ELI: http://data.europa.eu/eli/reg/2011/182/oj).	
Recital 38a			
49a		***(38a) Skilled personnel, that is able to reliably deliver the relevant cybersecurity services at highest standards, is imperative for the effective implementation of the European Cyber Shield and the Cybersecurity Emergency Mechanism. It is therefore concerning that the Union is faced with a talent gap, characterised by a shortage of skilled professionals, while facing a rapidly evolving threat landscape as acknowledged in the Commission communication of 18 April 2023 on the Cyber Skills Academy. It is important to bridge this talent gap by strengthening cooperation and coordination among the different stakeholders, including the private sector, academia, Member States, the Commission and ENISA to scale up and create synergies, in all territories, for the investment in education and training, the development of public-private partnerships, support of research and innovation initiatives, the development and mutual recognition of common standards and certification of cybersecurity skills, including through the European Cyber Security Skills Framework.***	

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
		This should also facilitate the mobility of cybersecurity professionals within the Union. This Regulation should aim to promote a more diverse cybersecurity workforce. All measures aiming to increase cybersecurity skills requires safeguards to avoid a 'brain drain' and a risk to labour mobility.	
Recital 38b			
49b		***(38b) The reinforcement of specialised, interdisciplinary and general skills and competences across the Union is needed, with a special focus on women, as the gender gap persists in cybersecurity with women comprising 20 % of the average worldwide presence. Women must be present and part of the design of the digital future and its governance.***	
Recital 38c			
49c		***(38c) Strengthening research and innovation (R&I) in cybersecurity is intended to increase the resilience and the open strategic autonomy of the Union. Similarly, it is important to create synergies with R&I programmes and with existing instruments and institutions and to strengthen cooperation and coordination among the different stakeholders, including the private sector, civil society, academia, Member States, the Commission and ENISA;***	

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
Recital 38d			
49d		***(38d) This Regulation should contribute to the commitment of the European Declaration on Digital Rights and Principles for the Digital Decade linked to protect the interests of our democracies, people, businesses and public institutions against cybersecurity risks and cybercrime including data breaches and identity theft or manipulation. The application of this Regulation should also contribute to improving the implementation of other legislation, for example on artificial intelligence, data privacy and data regulation in terms of cybersecurity and cyber resilience.***	
Recital 38e			
49e		***(38e) Increasing cybersecurity culture which comprehends security, including that of the digital environment, as a public good will be key for the successful implementation of this Regulation. Therefore, developing measures to include and increase citizens' awareness should be another means of guaranteeing the safeguard of our democracies and fundamental values.***	
Recital 38f			
49f			

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
		(38f) In order to supplement certain non-essential elements of this Regulation, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission to specify the conditions for interoperability between the Cross-border SOCs, establish the procedural arrangements for the information sharing between the Cross-border SOCs on the one hand and EU-CyCLONe, the CSIRTs network and the Commission on the other, specify the types and number of response services required for the EU Cybersecurity Reserve, and specify further the detailed arrangements for allocating the EU Cyersecurity Reserve support services. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making*. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.	
Recital 39			
50	(39) The objective of this Regulation can be	(39) ***Since the objectives*** ~~***The objective***~~ of this	(39) The objective of this Regulation can be

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
	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.	Regulation***, namely to reinforce the Union's cyber threat prevention, detection, response and recover capacities and to establish a general framework breaking up communication silo cannot be sufficiently achieved*** ~~*can be better achieved at Union level than*~~ by the Member States ***but can rather be better achieved at Union level***. 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. ***In accordance with the principle of proportionality, as set out in that Article,*** this Regulation does not go beyond what is necessary in order to achieve that objective~~.~~	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.
Formula			
51	HAVE ADOPTED THIS REGULATION:	HAVE ADOPTED THIS REGULATION:	HAVE ADOPTED THIS REGULATION:
Chapter I			
52	Chapter I GENERAL OBJECTIVES, SUBJECT MATTER, AND DEFINITIONS	Chapter I GENERAL OBJECTIVES, SUBJECT MATTER, AND DEFINITIONS	Chapter I GENERAL OBJECTIVES, SUBJECT MATTER, AND DEFINITIONS
Article 1			
53	Article 1 Subject-matter and objectives	Article 1 Subject-matter and objectives	Article 1 Subject-matter and objectives

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
Article 1(1)			
54	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:	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:	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:
Article 1(1), point (a)			
55	(a) the deployment of a pan-European infrastructure of Security Operations Centres ('European Cyber Shield') to build and enhance common detection and situational awareness capabilities;	(a) the deployment of a pan-European ~~*infrastructure*~~***network*** of Security Operations Centres ('European Cyber Shield') to build and enhance common detection and situational awareness capabilities;	(a) the ~~deployment~~**establishment** of a pan-European infrastructure of ~~Security Operations Centres~~ **Cyber Hubs** ('European **Cybersecurity Alert System** ~~Cyber Shield~~') to build and enhance ~~common~~**coordinated** detection and **common** situational awareness capabilities;
Article 1(1), point (b)			
56	(b) the creation of a Cybersecurity Emergency Mechanism to support Member States in preparing for, responding to, and immediate recovery from significant and large-scale cybersecurity incidents;	(b) the creation of a Cybersecurity Emergency Mechanism to support Member States in preparing for, responding to, and immediate recovery from significant and large-scale cybersecurity incidents;	(b) the creation of a Cybersecurity Emergency Mechanism to support Member States **and other users** in preparing for, responding to, ~~and immediate~~ **mitigating the impact of and initiating** recovery from significant**, large-scale** and large-scale **equivalent** cybersecurity incidents;
Article 1(1), point (c)			
57	(c) the establishment of a European	(c) the establishment of a European	(c) the establishment of a European

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
	Cybersecurity Incident Review Mechanism to review and assess significant or large-scale incidents.	Cybersecurity Incident Review Mechanism to review and assess significant or large-scale incidents.	Cybersecurity Incident Review Mechanism to review and assess significant or large-scale incidents.
Article 1(2)			
58	2. This Regulation pursues the objective to strengthen solidarity at Union level through following specific objectives:	2. This Regulation pursues the objective to strengthen solidarity at Union level through following specific objectives:	2. This Regulation pursues the objective ~~to strengthen~~**of strengthening** solidarity at Union level **and enhancing Member States cyber resilience, so as to reinforce the competitive position of industry and services sectors in the Union across the digital economy and contribute to the Union's technological sovereignty in the area of cybersecurity,** through **the** following specific objectives:
Article 1(2), point (a)			
59	(a) to strengthen common Union detection and situational awareness of cyber threats and incidents thus allowing to reinforce the competitive position of industry and services sectors in the Union across the digital economy and contribute to the Union's technological sovereignty in the area of cybersecurity;	(a) to strengthen common Union detection and situational awareness of cyber threats and incidents thus allowing ***support for the industrial capacity of the Union and the Member States in the cybersecurity sector, and*** to reinforce the competitive position of industry***, in particular microenterprises, SMEs including startups,*** and services sectors in the Union across the digital economy and ***to*** contribute to the Union's technological sovereignty ***its open strategic autonomy, competitiveness and and resilience in that sector, strengthening the cybersecurity ecosystem with a view to ensuring strong***	(a) to strengthen common **coordinated** Union detection **capacities and common**~~and~~ situational awareness of cyber threats and incidents thus allowing to reinforce the competitive position of industry and services sectors in the Union across the digital economy and contribute to the Union's technological sovereignty in the area of cybersecurity;

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
		Union capabilities, including in cooperation with international partners ~~*in the area of cybersecurity*~~;	
Article 1(2), point (b)			
60	(b) to reinforce preparedness of entities operating in critical and highly critical sectors across the Union and strengthen solidarity by developing common response capacities against significant or large-scale cybersecurity incidents, including by making Union cybersecurity incident response support available for third countries associated to the Digital Europe Programme ('DEP');	(b) to reinforce preparedness of entities operating in critical and highly critical sectors across the Union and strengthen solidarity by developing common response capacities against significant or large-scale cybersecurity incidents, including by making Union cybersecurity incident response support available for third countries associated to the Digital Europe Programme ('DEP');	(b) to reinforce preparedness of entities operating in ~~critical and highly~~**sectors of high criticality and other** critical sectors**,** across the Union and strengthen solidarity by developing ~~common response~~**enhanced response and recovery** capacities ~~against~~ **to handle** significant**, large-scale or large-scale-equivalent** ~~or large-scale~~ cybersecurity incidents, including ~~by~~**the possibility of** making Union cybersecurity incident response support available for **DEP-associated** third countries ~~associated to the Digital Europe Programme ('DEP')~~;
Article 1(2), point (c)			
61	(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..	(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..	(c) to enhance Union resilience and contribute to effective response by**, upon request of the Member States,** reviewing and assessing significant or large-scale incidents, including drawing lessons learned and, where appropriate, recommendations~~.~~**, with the approval of the Member States concerned**.
Article 1(2), point (ca)			

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
61a		***(ca) to develop, in a coordinated manner, skills, knowhow abilities and competencies of the workforce, with a view to ensuring cybersecurity and creating synergies with the Cybersecurity Skills Academy.***	
Article 1(2a)			
61b			**2a. The actions under this Regulation shall be conducted with due respect to the Member States' competences and shall be complementary to the activities carried out by the CSIRTs network, NIS Cooperation Group, and EU-CyCLONe.**
Article 1(3)			
62	3. This Regulation is without prejudice to the Member States' primary responsibility for national security, public security, and the prevention, investigation, detection and prosecution of criminal offences.	3. This Regulation is without prejudice to the Member States' primary responsibility for national security, public security, and the prevention, investigation, detection and prosecution of criminal offences.	3. This Regulation is without prejudice to the Member States' ~~primary responsibility for national security, public security, and the prevention, investigation, detection and prosecution of criminal offences~~**essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State**.
Article 1(3a)			
62a			

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
			4. This Regulation is without prejudice to Article 346 TFEU and all exchange of information that is confidential pursuant to Union or national rules shall be limited to that which is relevant and proportionate to the purpose of that exchange. The exchange of such information under this Regulation shall preserve the confidentiality of the information and protect the security and commercial interests of the entities concerned, in full respect of trade and business secrets. It shall not entail the supply of information the disclosure of which would be contrary to the Member States' essential interests of national security, public security or defence.
Article 2			
63	Article 2 Definitions	Article 2 Definitions	Article 2 Definitions
Article 2, first paragraph			
64	For the purposes of this Regulation, the following definitions apply:	For the purposes of this Regulation, the following definitions apply:	For the purposes of this Regulation, the following definitions apply:
Article 2, first paragraph, point (-1)			
64a		***(-1) 'National Security Operations Centre' or 'National SOC' means a centralised national***	

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
		capacity continuously gathering and analysing cyber threat intelligence information and improving the cybersecurity posture in accordance with Article 4;	
Article 2, first paragraph, point (-1)			
64b			**(-1) 'National Cyber Hub' means a single entity designated by and acting under the authority of a Member State, which may be a CSIRT, a national cyber crisis management authority or other competent authority designated or established under Directive 2022/2555 or another entity, under the authority of a Member State, which has the following functionalities:**
Article 2, first paragraph, point (-1a)			
64c			**(-1a) it has the capacity to act as a reference point and gateway to other public and private organisations at national level for collecting and analysing information on cyber threats and incidents and to contribute to a Cross Border Cyber Hub;**
Article 2, first paragraph, point (-1b)			
64d			**(-1b) it is capable of detecting, aggregating, and analysing data relevant to cyber threats and incidents by using in particular state-of-**

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
			the-art technologies;
Article 2, first paragraph, point (1)			
65	(1) 'Cross-border Security Operations Centre' ("Cross-border SOC") means a multi-country platform, that brings together in a coordinated network structure national SOCs from at least three Member States who form a Hosting Consortium, and that is designed to prevent cyber threats and incidents and to support the production of high-quality intelligence, notably through the exchange of data from various sources, public and private, as well as through the sharing of state-of-the-art tools and jointly developing cyber detection, analysis, and prevention and protection capabilities in a trusted environment;	(1) 'Cross-border Security Operations Centre' ~~("~~***or '*** Cross-border SOC~~")~~***'*** means a multi-country platform, that brings together in a coordinated network structure national SOCs ~~*from at least three Member States who form a Hosting Consortium, and that is designed to prevent cyber threats and incidents and to support the production of high-quality intelligence, notably through the exchange of data from various sources, public and private, as well as through the sharing of state-of-the-art tools and jointly developing cyber detection, analysis, and prevention and protection capabilities in a trusted environment*~~ ***in accordance with Article 5***;	(1) '~~Cross-border Security Operations Centre' ("Cross-border SOC")~~ **Cross-Border Cyber Hub'** means a multi-country platform, **established by a written consortium agreement** that brings together in a coordinated network structure National ~~SOCs~~**Cyber Hubs** from at least three Member States ~~who form a Hosting Consortium~~, and that is designed to ~~prevent~~**enhance the monitoring, detection and analysis of** cyber threats **to prevent** ~~and~~ incidents and to support the production of ~~high-quality~~ **cyber threat** intelligence, notably through the exchange of ~~data from various sources, public and private~~**relevant and, where appropriate, anonymised information**, 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 2, first paragraph, point (2)			
66	(2) 'public body' means a body governed by public law as defined in Article 2((1), point (4),), of Directive 2014/24/EU of the European Parliament and the Council[1];	(2) 'public body' means ~~*a body*~~***bodies*** governed by public law as defined in Article ~~*2((1)*~~***2(1)***, point (4)~~,~~), of Directive 2014/24/EU of the European Parliament and the Council[1];	(2) ~~'public body' means a body governed by public law as defined in Article 2((1), point (4),), of Directive 2014/24/EU of the European Parliament and the Council[1];~~
	1. Directive 2014/24/EU of the European Parliament and	1. ***[1]*** Directive 2014/24/EU of the European	~~1. Directive 2014/24/EU of the European Parliament and~~

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
	of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC (OJ L 94 28.3.2014, p. 65).	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).	~~of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC (OJ L 94 28.3.2014, p. 65).~~
Article 2, first paragraph, point (3)			
67	(3) 'Hosting Consortium' means a consortium composed of participating states, represented by National SOCs, that have agreed to establish and contribute to the acquisition of tools and infrastructure for, and operation of, a Cross-border SOC ;	(3) 'Hosting Consortium' means a consortium composed of participating states, represented by National SOCs, ~~*that have agreed to establish and contribute to the acquisition of tools and infrastructure for, and operation of, a Cross-border SOC*~~ ***in accordance with Article 5***;	(3) 'Hosting Consortium' means a consortium composed of participating ~~states, represented by National SOCs~~**Member States**,- that have agreed to establish and contribute to the acquisition of tools and infrastructure for, and operation of, a ~~Cross-border SOC ;~~**Cross Border Cyber Hub**
Article 2, first paragraph, point (3a)			
67a			**(3a) 'CSIRT' means a CSIRT designated or established pursuant to Article 10 of Directive (EU) 2022/2555.**
Article 2, first paragraph, point (4)			
68	(4) 'entity' means an entity as defined in Article 6, point (38), of Directive (EU) 2022/2555;	(4) 'entity' means an entity as defined in Article 6, point (38), of Directive (EU) 2022/2555;~~:~~	(4) 'entity' means an entity as defined in Article 6, point (38), of Directive (EU) 2022/2555;
Article 2, first paragraph, point (4a)			
68a		***(4a) 'critical entity' means critical entity as defined in Article 2, point (1), of Directive***	

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
		(EU) 2022/2557 of the European Parliament and of the Council[1]. ***1. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (OJ L 333, 27.12.2022, p. 164, ELI: http://data.europa.eu/eli/dir/2022/2557/oj).***	
Article 2, first paragraph, point (5)			
69	(5) 'entities operating in critical or highly critical sectors' means type of entities listed in Annex I and Annex II of Directive (EU) 2022/2555;	(5) 'entities operating in critical or highly critical sectors' means ~~*type of entities*~~***entities in the sectors*** listed in ~~*Annex*~~***Annexes*** I and ~~*Annex II of*~~***II to*** Directive (EU) 2022/2555;	(5) 'entities operating in ~~critical or highly~~**sectors of high criticality or other** critical sectors' means type of entities listed in Annex I and Annex II of Directive (EU) 2022/2555;
Article 2, first paragraph, point (5a)			
69a		***(5a) 'incident handling' means incident handling as defined in Article 6, point (8), of Directive (EU) 2022/2555;***	
Article 2, first paragraph, point (5b)			
69b		***(5b) 'risk' means risk as defined in Article 6, point (9), of Directive (EU) 2022/2555;***	
Article 2, first paragraph, point (6)			
70	(6) 'cyber threat' means a cyber threat as	(6) 'cyber threat' means a cyber threat as	(6) 'cyber threat' means a cyber threat as

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
	defined in Article 2, point (8), of Regulation (EU) 2019/881;	defined in Article 2, point (8), of Regulation (EU) 2019/881;	defined in Article 2, point (8), of Regulation (EU) 2019/881;
Article 2, first paragraph, point (6a)			
70a		***(6a) 'significant cyber threat' means a significant cyber threat as defined in Article 6, point (11), of Directive (EU) 2022/2555;***	
Article 2, first paragraph, point (6a)			
70b			**(6a) 'incident' means an incident as defined in Article 6, point (6), of Directive (EU) 2022/2555;**
Article 2, first paragraph, point (7)			
71	(7) 'significant cybersecurity incident' means a cybersecurity incident fulfilling criteria set out in Article 23(3) 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;	(7) 'significant cybersecurity incident' means a cybersecurity incident fulfilling criteria set out in Article 23(3) of Directive (EU) 2022/2555;
Article 2, first paragraph, point (8)			
72	(8) 'large-scale cybersecurity incident' means an incident as defined in Article 6, point (7) 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;	(8) 'large-scale cybersecurity incident' means an incident as defined in Article 6, point (7) of Directive (EU)2022/2555;
Article 2, first paragraph, point (8b)			
72a			

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
			(8b) 'large-scale-equivalent cybersecurity incident' means, in the case of Union institutions, bodies and agencies, a major incident as defined in Article 3 point (8) of Regulation (EU, Euratom) 2023/2841 of the European Parliament and the Council[1] and, in the case of DEP-associated third countries, an incident which causes a level of disruption that exceeds a DEP-associated third country's capacity to respond to it; _____ **1. Regulation (EU, Euratom) 2023/2841 of the European Parliament and of the Council of 13 December 2023 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union (OJ L, 2023/2841, 18.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2841/oj).**
Article 2, first paragraph, point (8c)			
72b			**(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;**
Article 2, first paragraph, point (8d)			
72c			**(8d) 'contracting authority' means the Commission or, to the extent that operation and administration of the EU Cybersecurity Reserve has been entrusted to ENISA under**

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
			Article 12(6) of this Regulation, ENISA.
Article 2, first paragraph, point (9)			
73	(9) 'preparedness' means a state of readiness and capability to ensure an effective rapid response to a significant or large-scale cybersecurity incident, obtained as a result of risk assessment and monitoring actions taken in advance;	(9) 'preparedness' means a state of readiness and capability to ensure an effective rapid response to a significant or large-scale cybersecurity incident, obtained as a result of risk assessment and monitoring actions taken in advance;	(9) ~~'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;~~
Article 2, first paragraph, point (10)			
74	(10) 'response' means action in the event of a significant or large-scale cybersecurity incident, or during or after such an incident, to address its immediate and short-term adverse consequences;	(10) 'response' means action in the event of a significant or large-scale cybersecurity incident, or during or after such an incident, to address its immediate and short-term adverse consequences;	(10) ~~'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;~~
Article 2, first paragraph, point (10a)			
74a		***(10a) 'managed security service provider' means a managed service provider as defined in Article 6, point (40), of Directive (EU) 2022/2555;***	
Article 2, first paragraph, point (11)			
75	(11) 'trusted providers' means managed security service providers as defined in Article	(11) 'trusted ***managed securiy service*** providers' means managed security service	(~~11~~**8a**) 'trusted providers' means managed security service providers as defined in Article

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
	6, point (40), of Directive (EU) 2022/2555 selected in accordance with Article 16 of this Regulation.	providers ~~*as defined in Article 6, point (40), of Directive (EU) 2022/2555 selected*~~***selected to be included in the EU Cybersecurity Reserve*** in accordance with Article 16 of this Regulation.	6, point (40), of Directive (EU) 2022/2555 selected in accordance with Article 16 of this Regulation.
Chapter II			
76	Chapter II THE EUROPEAN CYBER SHIELD	Chapter II THE EUROPEAN CYBER SHIELD	Chapter II THE EUROPEAN **CYBERSECURITY ALERT SYSTEM**~~CYBER SHIELD~~
Article 3			
77	Article 3 Establishment of the European Cyber Shield	Article 3 Establishment of the European Cyber Shield	Article 3 **Article 3** Establishment of the European ~~Cyber Shield~~**Cybersecurity Alert System**
Article 3(1), first subparagraph			
78	1. An interconnected pan-European infrastructure of Security Operations Centres ('European Cyber Shield') shall be established to develop advanced capabilities for the Union to detect, analyse and process data on cyber threats and incidents in the Union. It shall consist of all National Security Operations Centres ('National SOCs') and Cross-border Security Operations Centres ('Cross-border SOCs').	1. ~~*An interconnected pan-European infrastructure*~~***A network*** of Security Operations Centres ('European Cyber Shield') shall be established to develop advanced capabilities for the Union to detect, analyse and process data on cyber threats and ***prevent*** incidents in the Union. It shall consist of all National Security Operations Centres ('National SOCs') and Cross-border Security Operations Centres ('Cross-border SOCs').	1. ~~An interconnected~~**A** pan-European infrastructure **that consists of National Cyber Hubs and Cross Border**~~of Security Operations Centres ('European~~ Cyber ~~Shield')~~**Hubs joining on a voluntary basis, the European Cybersecurity Alert System** shall be established to ~~develop~~**support the development of** advanced capabilities for the Union to ~~detect, analyse and process~~**enhance detection, analysis and** data **processing**

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
			capabilities on cyber threats and incidents in the Union. ~~It shall consist of all National Security Operations Centres ('National SOCs') and Cross-border Security Operations Centres ('Cross-border SOCs').~~
Article 3(1), second subparagraph			
79	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.	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.	~~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.~~
Article 3(2), first subparagraph			
80	2. The European Cyber Shield shall:	2. The European Cyber Shield shall:	2. The European **Cybersecurity Alert System** ~~Cyber Shield~~ shall:
Article 3(2), first subparagraph, point (-a)			
80a			**(-a) contribute to better protection and response to cyber threats by supporting and cooperating with, and reinforcing the capacities of, relevant entities, in particular CSIRTs, the CSIRTs network, EU-CyCLONe and the competent authorities designated or established pursuant to Article 8 of Directive (EU) 2022/2555;**
Article 3(2), first subparagraph, point (a)			

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
81	(a) pool and share data on cyber threats and incidents from various sources through cross-border SOCs;	(a) pool and share data on cyber threats and incidents from various sources through Cross-border SOCs ***and where relevant exchange of information with CSIRTs Network***;	(a) pool ~~and share data~~**information** on cyber threats and incidents from various sources **within the Cross Border Cyber Hubs and share analysed or aggregated information** through ~~cross-border SOCs~~**Cross Border Cyber Hubs**;
Article 3(2), first subparagraph, point (b)			
82	(b) produce high-quality, actionable information and cyber threat intelligence, through the use of state-of-the art tools, notably Artificial Intelligence and data analytics technologies;	(b) produce high-quality, actionable information and cyber threat intelligence, through the use of state-of-the art tools, notably Artificial Intelligence and data analytics technologies;	(b) ~~produce~~**collect** high-quality, ~~actionable~~ information and cyber threat intelligence, through the use of state-of-the art tools **and advanced technologies , and share that information and cyber threat intelligence**~~, notably Artificial Intelligence and data analytics technologies~~;
Article 3(2), first subparagraph, point (c)			
83	(c) contribute to better protection and response to cyber threats;	(c) contribute to better protection and response to cyber threats***, including by providing concrete recommendations to entities***;	(c) ~~contribute to better protection and response to cyber threats;~~
Article 3(2), first subparagraph, point (d)			
84	(d) contribute to faster detection of cyber threats and situational awareness across the Union;	(d) contribute to faster detection of cyber threats and situational awareness across the Union;	(d) contribute to ~~faster~~**enhance coordinated** detection of cyber threats and **common** situational awareness across the Union**, and to the issuing of alerts**;

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
Article 3(2), first subparagraph, point (e)			
85	(e) provide services and activities for the cybersecurity community in the Union, including contributing to the development advanced artificial intelligence and data analytics tools.	(e) provide services and activities for the cybersecurity community in the Union, including contributing to the development ***of*** advanced artificial intelligence and data analytics tools.	(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.
Article 3(2), second subparagraph			
86	It shall be developed in cooperation with the pan-European High Performance Computing infrastructure established pursuant to Regulation (EU) 2021/1173.	It shall be developed in cooperation with the pan-European High Performance Computing infrastructure established pursuant to Regulation (EU) 2021/1173.	~~It shall be developed in cooperation with the pan-European High Performance Computing infrastructure established pursuant to Regulation (EU) 2021/1173.~~
Article 3(2a)			
86a			**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			
87	Article 4 National Security Operations Centres	Article 4 National Security Operations Centres	Article 4 National ~~Security Operations Centres~~**Cyber Hubs**

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
Article 4(1), first subparagraph			
88	1. In order to participate in the European Cyber Shield, each Member State shall designate at least one National SOC. The National SOC shall be a public body.	1. In order to ***be able to*** participate in the European Cyber Shield, each Member State shall designate at least one National SOC. The National SOC shall be a ***centralised capacity in a*** public body. ***When possible, the National SOCs shall be incorporated into the CSIRTs or other existing cybersecurity infrastructures and governance.***	1. ~~In order to~~ **Where a Member State decides to voluntarily** participate in the European **Cybersecurity Alert System, it** ~~Cyber Shield, each Member State~~ shall designate ~~at least one National SOC. The National SOC shall be a public body~~**a single National Cyber Hub exercising the functions as defined in Article 2 (-1) for the purposes of this Regulation**.
Article 4(1), second subparagraph			
89	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.	It shall have the capacity to act as a reference point and gateway to other public and private organisations at national level***, particularly their National SOCs,*** for collecting and analysing information on cybersecurity threats and incidents***, and, where relevant, sharing those information with members of the CSIRTs network of that Member State,*** and contributing to a Cross-border SOC. It shall be equipped with state-of-the-art technologies capable of ***preventing,*** detecting, aggregating, and analysing data relevant to cybersecurity threats and incidents.	~~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.~~
Article 4(1), second subparagraph a			
89a		***A National SOC or CSIRT may request telemetry, sensor or logging data of their***	

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
		national critical entities from managed security service providers that provide a service to the critical entity. That data shall be shared in accordance with Union data protection law and with the sole purpose of supporting the National SOC or CSIRT to the detect and prevent cybersecurity threats and incidents.	
Article 4(2)			
90	2. Following a call for expression of interest, National SOCs shall be selected by the European Cybersecurity Competence Centre ('ECCC') to participate in a joint procurement of tools and infrastructures with the ECCC. The ECCC may award grants to the selected National SOCs to fund the operation of those tools and infrastructures. The Union financial contribution shall cover up to 50% of the acquisition costs of the tools and infrastructures, and up to 50% of the operation costs, with the remaining costs to be covered by the Member State. Before launching the procedure for the acquisition of the tools and infrastructures, the ECCC and the National SOC shall conclude a hosting and usage agreement regulating the usage of the tools and infrastructures.	2. Following a call for expression of interest, National SOCs ~~*shall*~~***may*** be selected by the European Cybersecurity Competence Centre ('ECCC') to participate in a joint procurement of tools and infrastructures with the ECCC. The ECCC may award grants to the selected National SOCs to fund the operation of those tools and infrastructures. The Union financial contribution shall cover up to 50% of the acquisition costs of the tools and infrastructures, and up to 50% of the operation costs, with the remaining costs to be covered by the Member State. Before launching the procedure for the acquisition of the tools and infrastructures, the ECCC and the National SOC shall conclude a hosting and usage agreement regulating the usage of the tools and infrastructures.	2. ~~Following a call for expression of interest, National SOCs shall be selected by the European Cybersecurity Competence Centre ('ECCC') to participate in a joint procurement of tools and infrastructures with the ECCC. The ECCC may award grants to the selected National SOCs to fund the operation of those tools and infrastructures. The Union financial contribution shall cover up to 50% of the acquisition costs of the tools and infrastructures, and up to 50% of the operation costs, with the remaining costs to be covered by the Member State. Before launching the procedure for the acquisition of the tools and infrastructures, the ECCC and the National SOC shall conclude a hosting and usage agreement regulating the usage of the tools and infrastructures.~~
Article 4(3)			
91	3. A National SOC selected pursuant to paragraph 2 shall commit to apply to participate	3. A National SOC selected pursuant to paragraph 2 shall commit to apply to participate	3. A ~~National SOC~~ **Member State** selected pursuant to **Article 8a** paragraph ~~2~~**1** shall

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
	in a Cross-border SOC within two years from the date on which the tools and infrastructures are acquired, or on which it receives grant funding, whichever occurs sooner. If a National SOC is not a participant in a Cross-border SOC by that time, it shall not be eligible for additional Union support under this Regulation.	in a Cross-border SOC within two years from the date on which the tools and infrastructures are acquired, or on which it receives grant funding, whichever occurs sooner. If a National SOC is not a participant in a Cross-border SOC by that time, it shall not be eligible for additional Union support under this Regulation.	commit to apply ~~to participate in a Cross-border SOC within two years from the date on which the tools and infrastructures are acquired, or on which it receives grant funding, whichever occurs sooner. If a~~**for its** National ~~SOC is not a participant in a Cross-border SOC by that time, it shall not be eligible for additional Union support under this Regulation~~**Cyber Hub to participate in a Cross Border Cyber Hub**.
Article 5			
92	Article 5 Cross-border Security Operations Centres	Article 5 Cross-border Security Operations Centres	Article 5 Cross-border ~~Security Operations Centres~~**Cyber Hubs**
Article 5(1)			
93	1. A Hosting Consortium consisting of at least three Member States, represented by National SOCs, committed to working together to coordinate their cyber-detection and threat monitoring activities shall be eligible to participate in actions to establish a Cross-border SOC.	1. A Hosting Consortium consisting of at least three Member States, represented by National SOCs, committed to working together to coordinate their cyber-detection and threat monitoring activities shall be eligible to participate in actions to establish a Cross-border SOC. ***A Cross-border SOC shall be designed to detect and analyse cyber threats, prevent incidents and support the production of high-quality intelligence, in particular through the exchange of data from various sources, public and private, as well as through the sharing of state-of-the-art tools and by jointly developing cyber detection, analysis, prevention and***	1. A Hosting Consortium consisting of at least three Member States, ~~represented by National SOCs, committed to working~~ **committed to ensuring that their National Cyber Hubs work** together to coordinate their cyber-detection and threat monitoring activities shall be eligible to participate in actions to establish a ~~Cross-border SOC~~**Cross-Border Cyber Hub**.

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
		protection capabilities in a trusted and secure environment.	
Article 5(2)			
94	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.	2. Following a call for expression of interest, a Hosting Consortium ~~*shall*~~***may*** 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.	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.~~
Article 5(2a)			
94a		***2a. By way of derogation from Article 176 of Regulation (EU, Euratom) 2018/1046, entities established in third countries that are not parties to the GPA shall not participate in the joint procurement of tools and infrastructures.***	

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
Article 5(3)			
95	3. Members of the Hosting Consortium shall conclude a written consortium agreement which sets out their internal arrangements for implementing the hosting and usage Agreement.	3. Members of the Hosting Consortium shall conclude a written consortium agreement which sets out their internal arrangements for implementing the hosting and usage Agreement.	3. Members of the Hosting Consortium shall conclude a written consortium agreement which sets out their internal arrangements for implementing the hosting and usage agreement **referred to in Article 8a**.
Article 5(4)			
96	4. A Cross-border SOC shall be represented for legal purposes by a National SOC acting as coordinating SOC, or by the Hosing Consortium if it has legal personality. The co-ordinating SOC shall be responsible for compliance with the requirements of the hosting and usage agreement and of this Regulation.	4. A Cross-border SOC shall be represented for legal purposes by a National SOC acting as coordinating SOC, or by the Hosing Consortium if it has legal personality. The co-ordinating SOC shall be responsible for compliance with the requirements of the hosting and usage agreement and of this Regulation.	4. A ~~Cross-border SOC~~ **Cross-Border Cyber Hub** shall be represented for legal purposes by a ~~National SOC~~ **member of the Hosting Consortium** acting as ~~coordinating SOC~~**a coordinator** , or by the ~~Hosing~~**Hosting** Consortium if it has legal personality. ~~The co-ordinating SOC shall be responsible for compliance with the requirements of~~ **The responsibility for compliance of the Cross-Border Cyber Hub with this Regulation and** the hosting and usage agreement ~~and of this Regulation~~**shall be determined in the written consortium agreement referred to in paragraph 3**.
Article 6			
97	Article 6 Cooperation and information sharing within and between cross-border SOCs	Article 6 Cooperation and information sharing within and between cross-border SOCs	Article 6 Cooperation and information sharing within and between ~~cross-border SOCs~~**Cross-Border Cyber Hubs**

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
Article 6(1)			
98	1. Members of a Hosting Consortium shall exchange relevant information among themselves within the Cross-border SOC including information relating to cyber threats, near misses, vulnerabilities, techniques and procedures, indicators of compromise, adversarial tactics, threat-actor-specific information, cybersecurity alerts and recommendations regarding the configuration of cybersecurity tools to detect cyber attacks, where such information sharing:	1. Members of a Hosting Consortium shall exchange relevant information among themselves within the Cross-border SOC including information relating to cyber threats, near misses, vulnerabilities, techniques and procedures, indicators of compromise, adversarial tactics, threat-actor-specific information, cybersecurity alerts and recommendations regarding the configuration of cybersecurity tools to detect cyber attacks, where such information sharing:	1. Members of a Hosting Consortium shall ~~exchange relevant information among themselves within the Cross-border SOC including information relating to cyber threats, near misses, vulnerabilities, techniques and procedures, indicators of compromise, adversarial tactics, threat-actor-specific~~**ensure that their National Cyber Hubs exchange, in accordance with the Consortium Agreement referred to in Article 5(3), relevant and where appropriate, anonymised** information~~, cybersecurity alerts and recommendations regarding the configuration of cybersecurity tools to detect~~ **among themselves within the Cross-Border** Cyber ~~attacks,~~**Hub** where such information sharing:
Article 6(1), point (a)			
99	(a) aims to prevent, detect, respond to or recover from incidents or to mitigate their impact;	(a) ~~*aims to prevent, detect, respond to or recover from incidents or to mitigate their impact*~~***improves the exchange of cyber threat intelligence between National and Cross-border SOCs and industry ISACs with the aim to prevent, detect, or mitigate threats***;	(a) ~~aims to prevent, detect, respond to or recover from~~ **fosters and enhances the detection of cyber threats and reinforces the capabilities of the CSIRTs network to prevent and respond to** incidents or to mitigate their impact;
Article 6(1), point (b)			
100			

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
	(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.	(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.	(b) ~~enhances~~**enhance** 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 6(2)			
101	2. The written consortium agreement referred to in Article 5(3) shall establish:	2. The written consortium agreement referred to in Article 5(3) shall establish:	2. The written consortium agreement referred to in Article 5(3) shall establish:
Article 6(2), point (a)			
102	(a) a commitment to share a significant amount of data referred to in paragraph 1, and the conditions under which that information is to be exchanged;	(a) a commitment to share a significant ~~*amount of*~~ .data referred to in paragraph 1, and the conditions under which that information is to be exchanged;	(a) a commitment to share ~~a significant amount of data~~**among the members of the Consortium relevant and where appropriate, anonymised information** referred to in paragraph 1, and the conditions under which that information is to be exchanged**. The agreement may specify that the information shall be exchanged in accordance with national law**;
Article 6(2), point (b)			
103			

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
	(b) a governance framework incentivising the sharing of information by all participants;	(b) a governance framework incentivising the sharing of information by all participants;	(b) a governance framework **clarifying and** incentivising the sharing of **relevant and, where appropriate, anonymised** information **referred to in paragraph 1** by all participants;
Article 6(2), point (c)			
104	(c) targets for contribution to the development of advanced artificial intelligence and data analytics tools.	(c) targets for contribution to the development of advanced artificial intelligence and data analytics tools.	(c) targets for contribution to the development of advanced **tools and technologies, such as** artificial intelligence and data analytics tools.
Article 6(3)			
105	3. To encourage exchange of information between Cross-border SOCs, Cross-border SOCs shall ensure a high level of interoperability between themselves. To facilitate the interoperability between the Cross-border SOCs, the Commission may, by means of implementing acts, after consulting the ECCC, specify the conditions for this interoperability. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2) of this Regulation.	3. To encourage exchange of information ~~between~~***among*** Cross-border SOCs ***and with industry ISACs***, Cross-border SOCs shall ensure a high level of interoperability between themselves ***and, where possible, with industry ISACs***. To facilitate the interoperability between the Cross-border SOCs ***and with industry ISACs, information sharing standards and protocols may be harmonised with international standards and industry best practices. The joint procurement of cyber infrastructures, services and tools shall also be encouraged. Moreover*** ~~, the Commission may, by means of implementing acts~~, after consulting the ECCC~~, specify the conditions for this interoperability. Those implementing acts shall be adopted~~ ***and ENISA, the Commission is empowered, by... [six months from the date of entry into force of this Regulation] to adopt***	3. To encourage exchange of **relevant and, where appropriate, anonymised** information between ~~Cross-border SOCs, Cross-border SOCs~~**Cross-Border Cyber Hubs , Cross-Border Cyber Hubs** shall ensure a high level of interoperability between themselves. ~~To facilitate the interoperability between the Cross-border SOCs, the Commission may, by means of implementing acts, after consulting the ECCC, specify the conditions for this interoperability. Those implementing acts shall be adopted in accordance~~**Cross-Border Cyber Hubs shall conclude cooperation agreements with one another, specifying interoperability and information sharing principles among the Cross-Border Cyber Hubs. Cross-Border Cyber Hubs shall inform the Commission about the agreements concluded. ENISA, in cooperation** with the ~~examination procedure~~

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
		delegated acts in accordance with ***Article 20a to supplement this Regulation, by specifying the conditions for this interoperability in close coordination with the Cross-border SOCs and on the basis of international standards and industry best practices*** ~~*the examination procedure referred to in Article 21(2) of this Regulation*~~.	~~referred to in Article 21(2) of this Regulation~~**ECCC and the CSIRTs network may issue guidance to support establishing interoperability between the Cross-Border Cyber Hubs**.
Article 6(4)			
106	4. Cross-border SOCs shall conclude cooperation agreements with one another, specifying information sharing principles among the cross-border platforms.	4. Cross-border SOCs shall conclude cooperation agreements with one another ***and with, where appropriate, industry ISACs,***, specifying information sharing ***and interoperability*** principles among the cross-border platforms***, taking into consideration existing relevant information sharing mechanisms provided for in Directive (EU) 2022/2555. Where appropriate, Cross-border SOCs shall conclude cooperation agreements with industry ISACs. In the context of a potential or ongoing large-scale cybersecurity incident, information sharing mechanisms shall comply with the relevant provisions of the Directive (EU) 2022/2555***.	4. ~~Cross-border SOCs shall conclude cooperation agreements with one another, specifying information sharing principles among the cross-border platforms.~~
Article 7			
107	Article 7 Cooperation and information sharing with Union entities	Article 7 Cooperation and information sharing with ~~*Union entities*~~***the CSIRT network***	Article 7 Cooperation and information sharing with ~~Union entities~~ **Union-level networks**

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
Article 7(-1)			
107a			**-1. Cross-Border Cyber Hubs and the CSIRTs Network shall cooperate closely, in particular for the purpose of sharing information. To that end, they shall agree on procedural arrangements on cooperation and sharing of relevant information and, without prejudice to paragraph 1, the types of information to be shared.**
Article 7(1)			
108	1. Where the Cross-border SOCs obtain information relating to a potential or ongoing large-scale cybersecurity incident, they shall provide relevant information to EU=CyCLONe, the CSIRTs network and the Commission, in view of their respective crisis management roles in accordance with Directive (EU) 2022/2555 without undue delay.	1. Where the Cross-border SOCs obtain information relating to a potential or ongoing large-scale cybersecurity incident ***for the purpose of shared situation awareness, the coordinating SOC*** ~~*, they*~~ shall provide ***the*** relevant information to ~~*EU=CyCLONe*~~***its CSIRT or competent authority, which will report this to the EU-CyCLONe***, the CSIRTs network and the Commission ***and ENISA, in line with*** ~~*, in view of*~~ their respective crisis management roles ***and procedures*** in accordance with Directive (EU) 2022/2555 without undue delay. ***This paragraph shall not impose further obligations on public or private entities to communicate a potential or ongoing large-scale cybersecurity incident for the fulfilment of the obligations laid down in the Directive (EU) 2022/2555.***	1. Where the ~~Cross-border SOCs~~ **Cross-Border Cyber Hubs** obtain information relating to a potential or ongoing large-scale cybersecurity incident, they shall ~~provide~~**ensure that** relevant information ~~to EU=CyCLONe,~~**as well as early warnings are provided to** the CSIRTs network**, and EU-CyCLONe, without undue delay** ~~and the Commission~~, in view of their respective crisis management roles in accordance with Directive (EU) 2022/2555 ~~without undue delay~~.

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
Article 7(2)			
109	2. The Commission may, by means of implementing acts, determine the procedural arrangements for the information sharing provided for in paragraphs 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2) of this Regulation.	2. The Commission ~~*may, by means of implementing acts, determine*~~***is empowered to adopt delegated acts in accordance with Article 20a after consulting the CSIRT network to supplement this Regulation by determining*** the procedural arrangements for the information sharing provided for in paragraphs 1~~*. Those implementing acts shall be adopted*~~ ***of this Article and*** in accordance with ~~*the examination procedure referred to in Article 21(2) of this Regulation*~~***Directive (EU) 2022/2555***.	2. ~~The Commission may, by means of implementing acts, determine the procedural arrangements for the information sharing provided for in paragraphs 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2) of this Regulation.~~
Article 8			
110	Article 8 Security	Article 8 Security	Article 8 Security
Article 8(1)			
111	1. Member States participating in the European Cyber Shield shall ensure a high level of data security and physical security of the European Cyber Shield infrastructure, and shall ensure that the infrastructure shall be adequately managed and controlled in such a way as to protect it from threats and to ensure its security and that of the systems, including that of data exchanged through the infrastructure.	1. Member States participating in the European Cyber Shield shall ensure a high level of ***confidentiality and*** data security and physical security of the European Cyber Shield infrastructure, and shall ensure that the infrastructure shall be adequately managed and controlled in such a way as to protect it from threats and to ensure its security and that of the systems, including that of data exchanged	1. Member States participating in the European **Cybersecurity Alert System** ~~Cyber Shield~~ shall ensure a high level of **cybersecurity, including** data security**, as well as** ~~and~~ physical security of the European **Cybersecurity Alert System** ~~Cyber Shield~~ infrastructure, and shall ensure that the infrastructure ~~shall be~~ **is** adequately managed and controlled in such a way as to protect it

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
		through the infrastructure.	from threats and to ensure its security and that of the systems, including that of **information and** data exchanged through the infrastructure.
Article 8(2)			
112	2. Member States participating in the European Cyber Shield shall ensure that the sharing of information within the European Cyber Shield with entities which are not Member State public bodies does not negatively affect the security interests of the Union.	2. Member States participating in the European Cyber Shield shall ensure that the sharing of information within the European Cyber Shield with entities which are not Member State public bodies does not negatively affect the security interests of the Union.	2. Member States participating in the European **Cybersecurity Alert System** ~~Cyber Shield~~ shall ensure that the sharing of **relevant and, where appropriate, anonymised** information within the European **Cybersecurity Alert System with any entity other than a** ~~Cyber Shield with entities which are not Member State~~ public ~~bodies~~ **authority or body of a Member State** does not negatively affect the security interests of the Union **or the Member States**.
Article 8(3)			
113	3. The Commission may adopt implementing acts laying down technical requirements for Member States to comply with their obligation under paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2) of this Regulation. In doing so, the Commission, supported by the High Representative, shall take into account relevant defence-level security standards, in order to facilitate cooperation with military actors.	3. The Commission may adopt implementing acts laying down technical requirements for Member States to comply with their obligation under paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2) of this Regulation. ***They shall comply with Directives (EU) 2022/2555 and (EU) 2022/2557 . In its implementing acts*** ~~*In doing so*~~, the Commission, supported by the High Representative, shall take into account relevant defence-level security standards, in order to facilitate cooperation with military actors.	3. ~~The Commission may adopt implementing acts laying down technical requirements for Member States to comply with their obligation under paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2) of this Regulation. In doing so, the Commission, supported by the High Representative, shall take into account relevant defence-level security standards, in order to facilitate cooperation with military actors.~~

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
Article 8a			
113a			**Article 8a** **Funding of the European Cybersecurity Alert System**
Article 8a(1)			
113b			**1. Following a call for expression of interest, Member States intending to participate in the European Cybersecurity Alert System shall be selected by the European Cybersecurity Competence Centre ('ECCC') to take part in a joint procurement of tools, infrastructures and services with the ECCC, in order to set up National Cyber Hubs, as referred to in Article 4(1), or enhance capabilities of an existing one. The ECCC may award grants to the selected Member States to fund the operation of those tools, infrastructures and services. The Union financial contribution shall cover up to 50% of the acquisition costs of the tools, infrastructures and services, and up to 50% of the operation costs, with the remaining costs to be covered by the Member State. Before launching the procedure for the acquisition of the tools, infrastructures and services, the ECCC and the Member State shall conclude a hosting and usage agreement**

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
			regulating the usage of the tools, infrastructures and services.Following a call for expression of interest, Member States intending to participate in the European Cybersecurity Alert System shall be selected by the European Cybersecurity Competence Centre ('ECCC') to take part in a joint procurement of tools, infrastructures and services with the ECCC, in order to set up National Cyber Hubs, as referred to in Article 4(1), or enhance capabilities of an existing one. The ECCC may award grants to the selected Member States to fund the operation of those tools, infrastructures and services. The Union financial contribution shall cover up to 50% of the acquisition costs of the tools, infrastructures and services, and up to 50% of the operation costs, with the remaining costs to be covered by the Member State. Before launching the procedure for the acquisition of the tools, infrastructures and services, the ECCC and the Member State shall conclude a hosting and usage agreement regulating the usage of the tools, infrastructures and services.
Article 8a(2)			
113c			**2. If a Member State's National Cyber Hub is not a participant in a Cross-Border Cyber Hub within two years from the date on which the tools, infrastructures and services were acquired, or on which it received grant**

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
			funding, whichever occurred sooner, the Member State shall not be eligible for additional Union support under this Chapter until it has joined a Cross-Border Cyber Hub.
Article 8a(3)			
113d			**3. Following a call for expression of interest, a Hosting Consortium shall be selected by the ECCC to participate in a joint procurement of tools, infrastructures and services with the ECCC. The ECCC may award to the Hosting Consortium a grant to fund the operation of the tools, infrastructures and services. The Union financial contribution shall cover up to 75% of the acquisition costs of the tools, infrastructures and services, and up to 50% of the operation costs, with the remaining costs to be covered by the Hosting Consortium. Before launching the procedure for the acquisition of the tools, infrastructures and services, the ECCC and the Hosting Consortium shall conclude a hosting and usage agreement regulating the usage of the tools, infrastructures and services.**
Article 8a(4)			
113e			**3a. The ECCC shall prepare, at least every**

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
			two years, a mapping of the tools, infrastructures and services necessary to establish or enhance National Cyber Hubs and Cross-Border Cyber Hubs, and their availability, including from legal entities established or deemed to be established in Member States and controlled by Member States or by nationals of Member States. When preparing the mapping, the ECCC shall consult the CSIRTs Network, any existing Cross-border Cyber Hubs, ENISA and the Commission.
Chapter III			
G 114	Chapter III CYBER EMERGENCY MECHANISM	Chapter III CYBER EMERGENCY MECHANISM	Chapter III CYBER EMERGENCY MECHANISM G
Article 9			
G 115	Article 9 Establishment of the Cyber Emergency Mechanism	Article 9 Establishment of the Cyber Emergency Mechanism	Article 9 Establishment of the Cyber Emergency Mechanism G
Article 9(1)			
116	1. A Cyber Emergency Mechanism is established to improve the Union's resilience to major cybersecurity threats and prepare for and mitigate, in a spirit of solidarity, the short-term impact of significant and large-scale	1. A ~~Cyber~~***Cybersecurity*** 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	1. A Cyber Emergency Mechanism is established to ~~improve~~**support improvement of** the Union's resilience to~~ major cybersecurity~~ **cyber** threats and prepare for and mitigate, in a spirit of solidarity, the short-term impact of

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
	cybersecurity incidents (the 'Mechanism').	significant and large-scale cybersecurity incidents (the 'Mechanism').	significant**, large-scale and large-scale-equivalent** ~~and large-scale~~ cybersecurity incidents (the 'Mechanism').
Article 9(1a)			
116a			**1a. In the case of Member States, the actions provided under the Mechanism shall be provided upon request and shall be complementary to Member States' efforts and actions to prepare for, respond to and recover from cybersecurity incidents.**
Article 9(2)			
117	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.	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.	2. Actions implementing the Cyber Emergency Mechanism shall be supported by funding from ~~DEP~~ **the Digital Europe Program ('DEP')**and implemented in accordance with Regulation (EU) 2021/694 and in particular Specific Objective 3 thereof.
Article 9(2a)			
117a			**2a. The actions under the Cyber Emergency Mechanism shall be implemented primarily through the ECCC in accordance with Regulation (EU) 2021/887 of the European Parliament and of the Council with the exception of actions implementing the EU Cybersecurity Reserve as referred to in**

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
			Article 10(1)(b), which shall be implemented by the Commission and ENISA.
Article 10			
118	Article 10 Type of actions	Article 10 Type of actions	Article 10 Type of actions
Article 10(-1)			
118a			**-1. Member States may request to participate in the actions under the Mechanism.**
Article 10(1)			
119	1. The Mechanism shall support the following types of actions:	1. The Mechanism shall support the following types of actions:	1. The Mechanism shall support the following types of actions:
Article 10(1), point (a)			
120	(a) preparedness actions, including the coordinated preparedness testing of entities operating in highly critical sectors across the Union;	(a) preparedness actions, including the coordinated preparedness testing of entities operating in highly critical sectors across the Union;	(a) preparedness actions, ~~including the coordinated preparedness testing of entities operating in highly critical sectors across the Union;~~**namely;**
Article 10(1), point (aa)			
120a			**(i) the coordinated preparedness testing of**

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
			entities operating in sectors of high criticality across the Union as specified in Article 11;
Article 10(1), point (ab)			
120b			**(ii) other preparedness actions for entities operating in sectors of high criticality and other critical sectors, as specified in Article 11a;**
Article 10(1), point (b)			
121	(b) response actions, supporting response to and immediate recovery from significant and large-scale cybersecurity incidents, to be provided by trusted providers participating in the EU Cybersecurity Reserve established under Article 12;	(b) response actions, supporting response to and immediate recovery from significant and large-scale cybersecurity incidents, to be provided by trusted ***managed security service*** providers participating in the EU Cybersecurity Reserve established under Article 12;	(b) ~~response~~ actions~~,~~ supporting response to and ~~immediate~~ **initiating** recovery from significant**, large-scale and large-scale-equivalent** ~~and large-scale~~ cybersecurity incidents, to be provided by trusted providers participating in the EU Cybersecurity Reserve established under Article 12;
Article 10(1), point (c)			
122	(c) mutual assistance actions consisting of the provision of assistance from national authorities of one Member State to another Member State, in particular as provided for in Article 11(3), point (f), of Directive (EU) 2022/2555.	(c) mutual assistance actions consisting of the provision of assistance from national authorities of one Member State to another Member State, in particular as provided for in Article 11(3), point (f), of Directive (EU) 2022/2555.	(c) mutual assistance actions ~~consisting of the provision of assistance from national authorities of one Member State to another Member State, in particular as provided for~~**as specified** in Article ~~11(3), point (f), of Directive (EU) 2022/2555~~**16a**.
Article 11			

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
123	Article 11 Coordinated preparedness testing of entities	Article 11 Coordinated preparedness testing of entities	Article 11 Coordinated preparedness testing of entities
Article 11(-1)			
123a			**-3. The Mechanism shall support the voluntary coordinated preparedness testing of entities operating in sectors of high criticality.**
Article 11(-1a)			
123b			**-2. The coordinated preparedness testing may consist of preparedness activities, such as penetration testing, and threat assessment.**
Article 11(-1b)			
123c			**-1. Support for preparedness actions under this Article shall be provided to Member States primarily in the form of grants and under the conditions defined in paragraph 4 and in the relevant work programmes referred to in Article 24 of the Digital Europe Programme.**
Article 11(1)			
124	1. For the purpose of supporting the	1. For the purpose of supporting the	1. For the purpose of supporting the **voluntary**

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
	coordinated preparedness testing of entities referred to in Article 10(1), point (a), across the Union, the Commission, after consulting the NIS Cooperation Group and ENISA, shall identify the sectors, or sub-sectors, concerned, from the Sectors of High Criticality listed in Annex I to Directive (EU) 2022/2555 from which entities may be subject to the coordinated preparedness testing, taking into account existing and planned coordinated risk assessments and resilience testing at Union level.	coordinated preparedness testing of entities referred to in Article 10(1), point (a), across the Union, the Commission, after consulting the NIS Cooperation Group and ENISA, shall identify the sectors, or sub-sectors, concerned, from the Sectors of High Criticality listed in Annex I to Directive (EU) 2022/2555 from which entities may be subject to the coordinated preparedness testing~~, taking into account existing and planned coordinated risk assessments and resilience testing at Union level~~ ***in accordance with the arrangements established for the entities in the Sectors of High Criticality listed in Annex I to Directive (EU) 2022/2555***.	coordinated preparedness testing of entities referred to in Article 10(1), point (a) **(i)**, across the Union, **and with due respect to the Member States competences,** the Commission, after consulting the NIS Cooperation Group and ~~ENISA~~**EU-CyCLONe** , shall identify the sectors, or sub-sectors, concerned, from the Sectors of High Criticality listed in Annex I to Directive (EU) 2022/2555 ~~from~~**for** which ~~entities may be subject to the coordinated preparedness testing, taking into account existing and planned coordinated risk assessments and resilience testing at Union level~~**a call for proposals to award grants may be issued. The participation of Member States in those calls is voluntary**.
Article 11(1a)			
124a			**1a. When identifying the sectors or sub-sectors under paragraph 1, the Commission shall take into account coordinated risk assessments and resilience testing at Union level, and the results thereof.**
Article 11(2)			
125	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.	2. The NIS Cooperation Group in cooperation with the Commission, ENISA, and the High Representative, ***and the entities that are subject to coordinated preparedness testing pursuant to paragraph 1,*** shall develop common risk	2. The NIS Cooperation Group in cooperation with the Commission, **the High Representative and** ENISA, and**, within the remit of its mandate, EU-CyCLONe** ~~the High Representative~~, shall develop common risk

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
		scenarios and methodologies for the coordinated ***preparedness testing exercises, culminating in a concerted workplan. Entities subject to coordinated preparedness testing shall develop and implement a remediation plan that carries out the recommendations resulting from preparedness tests.*** ***The NIS Cooperation Group may inform the prioritisation of sectors, or sub-sectors for the coordinated preparedness*** testing exercises.	scenarios and methodologies for the coordinated testing exercises **under Article 10 (1), point (a) (i) of this Regulation and, where appropriate, for other preparedness actions under Article 10(1)(a)(ii)**.
Article 11a			
125a			**Article 11a** **Other preparedness actions**
Article 11a(1)			
125b			**1. The Mechanism shall also support preparedness actions not covered by Article 11 of this Regulation on Coordinated preparedness actions for entities. Such actions shall include preparedness actions for entities in sectors not identified for coordinated testing pursuant to Article 11. Such actions may support vulnerability monitoring, risk monitoring, exercises and trainings.**
Article 11a(2)			
125c			

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
			2. Support for preparedness actions under this Article, shall be provided to Member States upon request and primarily in the form of grants and under the conditions defined in the relevant work programmes referred to in Article 24 of Regulation (EU) 2021/694.
Article 12			
126	Article 12 Establishment of the EU Cybersecurity Reserve	Article 12 Establishment of the EU Cybersecurity Reserve	Article 12 Establishment of the EU Cybersecurity Reserve
Article 12(1)			
127	1. An EU Cybersecurity Reserve shall be established, in order to assist users referred to in paragraph 3, in responding or providing support for responding to significant or large-scale cybersecurity incidents, and immediate recovery from such incidents.	1. An EU Cybersecurity Reserve shall be established, in order to assist users referred to in paragraph 3, in responding or providing support for responding to significant or large-scale cybersecurity incidents, and immediate recovery from such incidents. ***Where it is apparent that the procured services cannot be fully used for the purposes of providing support for responding to significant or large-scale incidents, those services can exceptionally be converted to excercises or trainings for dealing with incidents, and provided to the users upon request, by the contracting authority.***	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**, large-scale, or large-scale-equivalent** ~~or large-scale~~ cybersecurity incidents, and ~~immediate~~ **initiating** recovery from such incidents.
Article 12(2)			

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
128	2. The EU Cybersecurity Reserve shall consist of incident response services from trusted providers selected in accordance with the criteria laid down in Article 16. The Reserve shall include pre-committed services. The services shall be deployable in all Member States.	2. The EU Cybersecurity Reserve shall consist of incident response services from trusted ***managed security service*** providers selected in accordance with the criteria laid down in Article 16. The ***EU Cybersecurity*** reserve shall include pre-committed services. The services shall be deployable in all Member States***, shall reinforce the Union's technological sovereignty, its open strategic autonomy, competitiveness and resilience in the cyber security sector including by boosting innovation in the Digital Single Market across the Union***.	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~~**may** include pre-committed services. The **pre-committed** services **of a trusted provider shall be convertible, in cases where those services are not used for incident response during the time for which those services are pre-committed, into preparedness services related to incident prevention and response. The Reserve** shall be deployable **upon request** in all Member States**, Union institutions, bodies and agencies and in DEP-associated third countries referred to in Article 17(1)**.
Article 12(3)			
129	3. Users of the services from the EU Cybersecurity Reserve shall include:	3. Users of the services from the EU Cybersecurity Reserve shall include:	3. **The** users of the services from the EU Cybersecurity Reserve shall ~~include~~**be the following**:
Article 12(3), point (a)			
130	(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;	(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;	(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;
Article 12(3), point (b)			

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
131	(b) Union institutions, bodies and agencies.	(b) Union institutions, bodies and agencies ***as referred to in Article 3 (1) of the Regulation (EU) .../2023 of the European Parliament and of the Council[1] and CERT-EU.*** ***1. Regulation (EU) .../2023 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union (OJ C , , p, , ELI: ...).***	(b) ~~Union institutions, bodies and agencies~~**CERT-EU , in accordance with Article 13 of Regulation (EU, Euratom) 2023/2841**.
Article 12(3), point (ba)			
131a			**(c) Competent authorities such as Computer Security Incident Response Teams and cyber crisis management authorities of DEP-associated third countries in accordance with Article 17(3).**
Article 12(4)			
132	4. Users referred to in paragraph 3, point (a), shall use the services from the EU Cybersecurity Reserve in order to respond or support response to and immediate recovery from significant or large-scale incidents affecting entities operating in critical or highly critical sectors.	4. Users referred to in paragraph 3, point (a), shall use the services from the EU Cybersecurity Reserve in order to respond or support response to and immediate recovery from significant or large-scale incidents affecting entities operating in critical or highly critical sectors.	4. ~~Users referred to in paragraph 3, point (a), shall use the services from the EU Cybersecurity Reserve in order to respond or support response to and immediate recovery from significant or large-scale incidents affecting entities operating in critical or highly critical sectors.~~
Article 12(5)			
133			

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
	5. The Commission shall have overall responsibility for the implementation of the EU Cybersecurity Reserve. The Commission shall determine the priorities and evolution of the EU Cybersecurity Reserve, in line with the requirements of the users referred to in paragraph 3, and shall supervise its implementation, and ensure complementarity, consistency, synergies and links with other support actions under this Regulation as well as other Union actions and programmes.	5. The Commission shall have overall responsibility for the implementation of the EU Cybersecurity Reserve. The Commission shall determine the priorities and evolution of the EU Cybersecurity Reserve ***in coordination with the NIS2 Coordination Group and***, 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.	5. The Commission ~~shall have overall responsibility for the implementation of the EU Cybersecurity Reserve. The Commission~~**, in cooperation with EU CyCLONe, ENISA and the NIS Cooperation Group,** shall determine the priorities and evolution of the EU Cybersecurity Reserve, in line with the requirements of the users referred to in paragraph 3, and shall supervise its implementation, and ensure complementarity, consistency, synergies and links with other support actions under this Regulation as well as other Union actions and programmes. **These priorities shall be revised every two years.**
Article 12(6)			
134	6. The Commission may entrust the operation and administration of the EU Cybersecurity Reserve, in full or in part, to ENISA, by means of contribution agreements.	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.	6. The Commission may entrust the operation and administration of the EU Cybersecurity Reserve, in full or in part, to ENISA, by means of contribution agreements.
Article 12(7)			
135	7. In order to support the Commission in establishing the EU Cybersecurity Reserve, ENISA shall prepare a mapping of the services needed, after consulting Member States and the Commission. ENISA shall prepare a similar mapping, after consulting the Commission, to identify the needs of third countries eligible for support from the EU Cybersecurity Reserve	7. In order to support the Commission in establishing the EU Cybersecurity Reserve, ENISA shall prepare a mapping of the services needed, ***including the needed skills and capacity of the cybersecurity workforce,*** after consulting Member States and the Commission, ***and where appropriate, managed security services providers, and other cybersecurity***	7. ~~In order to support the Commission in establishing the EU Cybersecurity Reserve, ENISA shall prepare a mapping of the services needed, after consulting~~**ENISA shall prepare, at least every two years, a mapping of the services needed by the users as referred to in paragraph 3 points (a) and (b) and their availability, including from legal entities**

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
	pursuant to Article 17. The Commission, where relevant, shall consult the High Representative.	***industry representatives***. ENISA shall prepare a similar mapping, after consulting the Commission, ***managed security services providers, and where appropriate, other cybersecurity industry representatives*** 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 ***and inform the Council about the needs of third countries***.	**established or deemed to be established in** Member States and **controlled by Member States or by nationals of Member States. When preparing the mapping, ENISA shall consult the NIS Cooperation Group, EU-CyCLONe,** the Commission **and, where applicable, the Interinstitutional Cybersecurity Board**. ENISA shall prepare a similar mapping, after consulting **EU-CyCLONe and** the Commission~~, to identify the needs of third countries eligible for support from the EU Cybersecurity Reserve pursuant to Article 17. The Commission~~ **and informing the the Council, to identify the needs of users referred to in paragraph 3 point (c). ENISA**, where relevant, shall consult the High Representative.
Article 12(8)			
136	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).	8. The Commission ~~*may, by means of implementing*~~***is empowered to adopt delegated*** acts, ~~*specify*~~***in accordance with Article 20a to supplement this Regulation by specifying*** 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).*~~	8. The Commission may, by means of implementing acts, specify the types and the number of response services required for the EU Cybersecurity Reserve. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2). **When preparing those implementing acts, the Commission shall take into account the mapping referred to in paragraph 7. Before submitting those draft implementing acts to the committee referred to in Article 21(1), the Commission shall exchange advice and cooperate with the**

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
			NIS Cooperation Group and ENISA.
Article 13			
137	Article 13 Requests for support from the EU Cybersecurity Reserve	Article 13 Requests for support from the EU Cybersecurity Reserve	Article 13 Requests for support from the EU Cybersecurity Reserve
Article 13(1)			
138	1. The users referred to in Article 12(3) may request services from the EU Cybersecurity Reserve to support response to and immediate recovery from significant or large-scale cybersecurity incidents.	1. The users referred to in Article 12(3) may request services from the EU Cybersecurity Reserve to support response to and immediate recovery from significant or large-scale cybersecurity incidents.	1. The users referred to in Article 12(3) may request services from the EU Cybersecurity Reserve to support response to and ~~immediate~~**initiate** recovery from significant**, large-scale or large-scale-equivalent** ~~or large-scale~~ cybersecurity incidents.
Article 13(2)			
139	2. To receive support from the EU Cybersecurity Reserve, the users referred to in Article 12(3) shall take measures to mitigate the effects of the incident for which the support is requested, including the provision of direct technical assistance, and other resources to assist the response to the incident, and immediate recovery efforts.	2. To receive support from the EU Cybersecurity Reserve, the users referred to in Article 12(3) shall take measures to mitigate the effects of the incident for which the support is requested, including the provision of direct technical assistance, and other resources to assist the response to the incident, and immediate recovery efforts.	2. To receive support from the EU Cybersecurity Reserve, the users referred to in Article 12(3) shall take **all appropriate** measures to mitigate the effects of the incident for which the support is requested, including**, where relevant,** the provision of direct technical assistance, and other resources to assist the response to the incident, and ~~immediate~~ recovery efforts.
Article 13(3)			

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
140	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.	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.	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.~~**contracting authority in the following way:**
Article 13(3a)			
140a			**(a). In the case of users referred to in Article 12(3), point (a), of this Regulation, such requests shall be transmitted via the Single Point of Contact designated or established by the Member State in accordance with Article 8(3) of Directive (EU) 2022/2555.**
Article 13(3b)			
140b			**(b). In the case of the user referred to in Article 12(3), point (b), of this Regulation such requests shall be transmitted by CERT-EU.**
Article 13(3c)			
140c			**(c). In the case of users referred to in Article 12(3), point (c), of this Regulation, such requests shall be transmitted via the single**

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
			point of contact referred to in Article 17(4) of this Regulation.
Article 13(4)			
141	4. Member States shall inform the CSIRTs network, and where appropriate EU-CyCLONe, about their requests for incident response and immediate recovery support pursuant to this Article.	4. Member States shall inform the CSIRTs network, and where appropriate EU-CyCLONe, about their requests for incident response and immediate recovery support pursuant to this Article.	4. **In the case of requests from users referred to in Article 12(3), point (a), of this Regulation,** Member States shall inform the CSIRTs network, and where appropriate EU-CyCLONe, about their **users'** requests for incident response and ~~immediate~~ **initial** recovery support pursuant to this Article.
Article 13(5)			
142	5. Requests for incident response and immediate recovery support shall include:	5. Requests for incident response and immediate recovery support shall include:	5. Requests for incident response and ~~immediate~~ **initial** recovery support shall include:
Article 13(5), point (a)			
143	(a) appropriate information regarding the affected entity and potential impacts of the incident and the planned use of the requested support, including an indication of the estimated needs;	(a) appropriate information regarding the affected entity and potential impacts of the incident and the planned use of the requested support, including an indication of the estimated needs;	(a) appropriate information regarding the affected entity and potential impacts of the incident ~~and the planned use of the requested support, including an indication of the estimated needs;~~**on:**
Article 13(5), point (aa)			
143a			**(i) affected Member State(s) and users,**

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
			including the risk of spill over to another Member State, in the case of users referred to in Article 12(3), point (a), of this Regulation;
Article 13(5), point (ab)			
143b			**(ii) affected Union institutions, bodies and agencies, in the case of users referred to in Article 12(3), point (b), of this Regulation;**
Article 13(5), point (ac)			
143c			**(iii) affected DEP-associated countries, in the case of users referred to in Article 12(3), point (c), of this Regulation;**
Article 13(5), point (ad)			
143d			**(aa) information regarding the requested service, including the planned use of the requested support,including an indication of the estimated needs.**
Article 13(5), point (b)			
144	(b) information about measures taken to mitigate the incident for which the support is requested, as referred to in paragraph 2;	(b) information about measures taken to mitigate the incident for which the support is requested, as referred to in paragraph 2;	(b) **appropriate** information about measures taken to mitigate the incident for which the support is requested, as referred to in paragraph 2;

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
Article 13(5), point (c)			
145	(c) information about other forms of support available to the affected entity, including contractual arrangements in place for incident response and immediate recovery services, as well as insurance contracts potentially covering such type of incident.	(c) information about other forms of support available to the affected entity, including contractual arrangements in place for incident response and immediate recovery services, as well as insurance contracts potentially covering such type of incident.	(c) **where relevant, available** information about other forms of support available to the affected entity~~, including contractual arrangements in place for incident response and immediate recovery services, as well as insurance contracts potentially covering such type of incident~~.
Article 13(5a)			
145a			**5a. The information provided in accordance with paragraph 5 of this Article shall be handled in accordance with Union law while preserving the security and commercial interests of the entity concerned.**
Article 13(6)			
146	6. ENISA, in cooperation with the Commission and the NIS Cooperation Group, shall develop a template to facilitate the submission of requests for support from the EU Cybersecurity Reserve.	6. ENISA, in cooperation with the Commission and the NIS Cooperation Group, shall develop a template to facilitate the submission of requests for support from the EU Cybersecurity Reserve.	6. ENISA, in cooperation with the Commission and **EU-CyCLONe** ~~the NIS Cooperation Group~~, shall develop a template to facilitate the submission of requests for support from the EU Cybersecurity Reserve.
Article 13(7)			
147	7. The Commission may, by means of	7. The Commission ~~*may, by means of*~~	7. ~~The Commission may, by means of~~

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
	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).	~~*implementing*~~***is empowered to adopt delegated*** acts, ~~*specify*~~***in accordance with Article 20a to supplement this Regulation by specifying*** 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).*~~	~~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			
148	Article 14 Implementation of the support from the EU Cybersecurity Reserve	Article 14 Implementation of the support from the EU Cybersecurity Reserve	Article 14 Implementation of the support from the EU Cybersecurity Reserve
Article 14(1)			
149	1. Requests for support from the EU Cybersecurity Reserve, shall be assessed by the Commission, with the support of ENISA or as defined in contribution agreements under Article 12(6), and a response shall be transmitted to the users referred to in Article 12(3) without delay.	1. Requests for support from the EU Cybersecurity Reserve, shall be assessed by the Commission, with the support of ENISA or as defined in contribution agreements under Article 12(6), and a response shall be transmitted to the users referred to in Article 12(3) without ***undue*** delay ***and in any event within 24 hours***.	1. **In the case of requests from users referred to in Article 12(3)(a) and (b),** requests for support from the EU Cybersecurity Reserve, shall be assessed by the ~~Commission, with the support of ENISA or as defined in contribution agreements under Article 12(6), and a response shall be transmitted to the users referred to in Article 12(3) without delay~~**contracting authority A response shall be transmitted to the users referred to in Article 12(3)(a) and (b) without delay and in any event no later than 72 hours from the submission of the request to ensure effectiveness of the support action. The contracting authority may consult EU-CyCLONe during the assessment**

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
			process. It shall inform the Council and the Commission of the results of the process.
Article 14(1a)			
149a			**1a. The contracting authority shall ensure the confidentiality of the information shared in the course of requesting and providing the services. The contracting authority shall not share the information with others where further distribution of that information has been excluded by means of a visible marking applied by a user, unless the user explicitly authorises such sharing.**
Article 14(2)			
150	2. To prioritise requests, in the case of multiple concurrent requests, the following criteria shall be taken into account, where relevant:	2. To prioritise requests, in the case of multiple concurrent requests, the following criteria shall be taken into account, where relevant:	2. To prioritise requests, in the case of multiple concurrent requests **from users referred to in Article 12(3)**, the following criteria shall be taken into account, where relevant:
Article 14(2), point (a)			
G 151	(a) the severity of the cybersecurity incident;	(a) the severity of the cybersecurity incident;	(a) the severity of the cybersecurity incident; G
Article 14(2), point (b)			
G 152	(b) the type of entity affected, with higher priority given to incidents affecting essential	(b) the type of entity affected, with higher priority given to incidents affecting essential	(b) the type of entity affected, with higher priority given to incidents affecting essential G

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
	entities as defined in Article 3(1) of Directive (EU) 2022/2555;	entities as defined in Article 3(1) of Directive (EU) 2022/2555;	entities as defined in Article 3(1) of Directive (EU) 2022/2555;
Article 14(2), point (c)			
153	(c) the potential impact on the affected Member State(s) or users;	(c) the potential impact on the affected Member State(s) or users;	(c) the potential impact on the affected Member State(s) or users;
Article 14(2), point (d)			
154	(d) the potential cross-border nature of the incident and the risk of spill over to other Member States or users;	(d) the ***scale and*** potential cross-border nature of the incident and the risk of spill over to other Member States or users;	(d) the potential cross-border nature of the incident and the risk of spill over to other Member States or users;
Article 14(2), point (e)			
155	(e) the measures taken by the user to assist the response, and immediate recovery efforts, as referred in Article 13(2) and Article 13(5), point (b).	(e) the measures taken by the user to assist the response, and immediate recovery efforts, as referred in Article 13(2) and Article 13(5), point (b).	(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).
Article 14(2), point (ea)			
155a			**(f) the category of user under Article 12(3) of this Regulation, with higher priority given to Member State users, then to Union institutions, bodies and agencies and finally to DEP-associated third countries.**
Article 14(2a)			

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
155b			**Where operation and administration of the EU Cybersecurity Reserve has been entrusted, in full or in part, to ENISA under Article 12(6) of this Regulation, ENISA and Commission shall closely cooperate to prioritise requests in line with this paragraph.**
Article 14(3)			
156	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.	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 ***and any other provisions the parties to the agreement deem necessary for the provision of the respective service***.	3. The EU Cybersecurity Reserve services shall be provided in accordance with specific agreements between the ~~service~~ **trusted** provider and the user to which the support under the EU Cybersecurity Reserve is provided. Those **services may be provided in accordance with specific** agreements **between the trusted provider, the user and the affected entity. All agreements referred to in this paragraph** shall include liability conditions.
Article 14(4)			
157	4. The agreements referred to in paragraph 3 may be based on templates prepared by ENISA, after consulting Member States.	4. The agreements referred to in paragraph 3 ~~*may*~~***shall*** be based on templates prepared by ENISA, after consulting Member States ***and, where appropriate, other users of the EU Cybersecurity Reserve***.	4. The agreements referred to in paragraph 3 may be based on templates prepared by ENISA, after consulting Member States.

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
Article 14(5)			
158	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.	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***, except in cases of gross negligence in the evaluation of the application of the service provider or in case where the Commission or ENISA are users of the EU Cybersecurity Reserve according to Article 14 (3)***.	5. The Commission**, ENISA, and the users of the Reserve** ~~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.
Article 14(5a)			
158a			**5a. Users may use the EU Cybersecurity Reserve services provided in response to a request under Article 13(1) of this Regulation only in order to support response to and initiate recovery from significant incidents, large-scale cybersecurity incidents or large-scale-equivalent cybersecurity incidents. They may use those services only in respect of :**
Article 14(5b)			
158b			**(a). entities operating in sectors of high criticality or other critical sectors, in the case of users referred to in Article 12(3), points (a) and (c); and**

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
Article 14(5c)			
158c			**(b). Union institutions, bodies and agencies, in the case of the user referred to in Article 12 (3), point (b).**
Article 14(6)			
159	6. Within one month from the end of the support action, the users shall provide Commission and ENISA with a summary report about the service provided, results achieved and the lessons learned. When the user is from a third country as set out in Article 17, such report shall be shared with the High Representative.	6. Within one month from the end of the support action, the users shall provide Commission and ENISA ***CSIRTs Network and, where relevant, 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. ***The report shall respect Union and national law concerning the protection of sensitive or classified information.***	6. Within ~~one month~~**three months** from the end of ~~the~~ **a** support action, ~~the users shall provide Commission and ENISA with~~**any user that has received support shall provide** 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.~~ **as follows:**
Article 14(6a)			
159a			**(a). users referred to in Article 12(3), point (a), of this Regulation shall provide the summary report to the Commission, ENISA, the CSIRTs network and EU-CyCLONe**
Article 14(6b)			

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
159b			**(b). users referred to in Article 12(3), point (b), of this Regulation shall provide the summary report to the Commission, ENISA and the IICB.**
Article 14(6c)			
159c			**(c). users referred to in Article 12 (3) (c) of this Regulation shall share this report with the Commission, which will share it with the Council and the High Representative.**
Article 14(7)			
160	7. The Commission shall report to the NIS Cooperation Group about the use and the results of the support, on a regular basis.	7. The Commission shall report ***on a regular basis and at least twice a year*** to the NIS Cooperation Group about the use and the results of the support***. It shall protect confidential information, in accordance with Union and national law concerning the protection of sensitive or classified information***~~, on a regular basis~~.	7. **In case of users referred in Article 12 (3) (a) and (b) the contracting authority**~~The Commission~~ shall report to the NIS Cooperation Group**, on a regular basis and at least twice per year,** about the use and the results of the support~~, on a regular basis.~~ **.**
Article 14(7a)			
160a			**7a. In case of users referred to in Article 12 (3) (c), the Commission shall report to the Council and inform the High Representative on a regular basis and at least twice per year, about the use and the results of the support.**

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
Article 15			
161	Article 15 Coordination with crisis management mechanisms	Article 15 Coordination with crisis management mechanisms	Article 15 ~~Coordination with crisis management mechanisms~~
Article 15(1)			
162	1. In cases where significant or large-scale cybersecurity incidents originate from or result in disasters as defined in Decision 1313/2013/EU[1], the support under this Regulation for responding to such incidents shall complementactions under and without prejudice to Decision 1313/2013/EU. _____ 1. Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism (OJ L 347, 20.12.2013, p. 924).	1. In cases where significant or large-scale cybersecurity incidents originate from or result in disasters as defined in Decision 1313/2013/EU[1], the support under this Regulation for responding to such incidents shall complementactions under and without prejudice to Decision 1313/2013/EU. _____ 1. Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism (OJ L 347, 20.12.2013, p. 924).	1. ~~In cases where significant or large-scale cybersecurity incidents originate from or result in disasters as defined in Decision 1313/2013/EU[1], the support under this Regulation for responding to such incidents shall complementactions under and without prejudice to Decision 1313/2013/EU.~~ _____ ~~1. Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism (OJ L 347, 20.12.2013, p. 924).~~
Article 15(2)			
163	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.	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.	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.~~

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
Article 15(3)			
164	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.	3. In consultation with the High Representative, support under the ~~*Cyber*~~***Cybersecurity*** 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*~~***TFEU***.	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.~~
Article 15(4)			
165	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.	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.	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			
G 166	Article 16 Trusted providers	Article 16 Trusted providers	Article 16 Trusted providers G
Article 16(1)			
G 167			G

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
	1. In procurement procedures for the purpose of establishing the EU Cybersecurity Reserve, the contracting authority shall act in accordance with the principles laid down in the Regulation (EU, Euratom) 2018/1046 and in accordance with the following principles:	1. In procurement procedures for the purpose of establishing the EU Cybersecurity Reserve, the contracting authority shall act in accordance with the principles laid down in the Regulation (EU, Euratom) 2018/1046 and in accordance with the following principles:	1. In procurement procedures for the purpose of establishing the EU Cybersecurity Reserve, the contracting authority shall act in accordance with the principles laid down in the Regulation (EU, Euratom) 2018/1046 and in accordance with the following principles:
Article 16(1), point (a)			
168	(a) ensure the EU Cybersecurity Reserve includes services that may be deployed in all Member States, taking into account in particular national requirements for the provision of such services, including certification or accreditation;	(a) ensure the EU Cybersecurity Reserve includes services that may be deployed in all Member States, taking into account in particular national requirements for the provision of such services, including certification or accreditation;	(a) ensure **that the services included in** the EU Cybersecurity Reserve**, when taken as a whole, are such that the Reserve** ~~includes services that~~ may be deployed in all Member States, taking into account in particular national requirements for the provision of such services, including certification or accreditation;
Article 16(1), point (b)			
169	(b) ensure the protection of the essential security interests of the Union and its Member States.	(b) ensure the protection of the essential security interests of the Union and its Member States.	(b) ensure the protection of the essential security interests of the Union and its Member States~~.~~**;**
Article 16(1), point (c)			
170	(c) ensure that the EU Cybersecurity Reserve brings EU added value, by contributing to the objectives set out in Article 3 of Regulation (EU) 2021/694, including promoting the development of cybersecurity skills in the EU.	(c) ensure that the EU Cybersecurity Reserve brings EU added value, by contributing to the objectives set out in Article 3 of Regulation (EU) 2021/694, including promoting the development of cybersecurity skills in the EU***, and the achievement of gender balance in the***	(c) ensure that the EU Cybersecurity Reserve brings EU added value, by contributing to the objectives set out in Article 3 of Regulation (EU) 2021/694, including promoting the development of cybersecurity skills in the EU.

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
		sector, and reinforcing the Union's technological sovereignty, open strategic autonomy, competitiveness and resilience.	
Article 16(2)			
171	2. When procuring services for the EU Cybersecurity Reserve, the contracting authority shall include in the procurement documents the following selection criteria:	2. When procuring services for the EU Cybersecurity Reserve, the contracting authority shall include in the procurement documents the following selection criteria:	2. When procuring services for the EU Cybersecurity Reserve, the contracting authority shall include in the procurement documents the following selection criteria:
Article 16(2), point (a)			
172	(a) the provider shall demonstrate that its personnel has the highest degree of professional integrity, independence, responsibility, and the requisite technical competence to perform the activities in their specific field, and ensures the permanence/continuity of expertise as well as the required technical resources;	(a) the provider shall demonstrate that its personnel has the highest degree of professional integrity, independence, responsibility, and the requisite technical competence to perform the activities in their specific field, and ensures the permanence/continuity of expertise as well as the required technical resources;	(a) the provider shall demonstrate that its personnel has the highest degree of professional integrity, independence, responsibility, and the requisite technical competence to perform the activities in their specific field, and ensures the permanence/continuity of expertise as well as the required technical resources;
Article 16(2), point (b)			
173	(b) the provider, its subsidiaries and subcontractors shall have in place a framework to protect sensitive information relating to the service, and in particular evidence, findings and reports, and is compliant with Union security rules on the protection of EU classified information;	(b) the provider, its subsidiaries and subcontractors shall have in place a framework to protect sensitive information relating to the service, and in particular evidence, findings and reports, and is compliant with Union security rules on the protection of EU classified information;	(b) the provider, its subsidiaries and subcontractors shall have in place a framework**, including agreements where relevant,** to protect sensitive information relating to the service, and in particular evidence, findings and reports, and is compliant with Union security rules on the protection of EU classified information;

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
Article 16(2), point (c)			
174	(c) the provider shall provide sufficient proof that its governing structure is transparent, not likely to compromise its impartiality and the quality of its services or to cause conflicts of interest;	(c) the provider shall provide sufficient proof that its governing structure is transparent, not likely to compromise its impartiality and the quality of its services or to cause conflicts of interest;	(c) the provider shall provide sufficient proof that its governing structure is transparent, not likely to compromise its impartiality and the quality of its services or to cause conflicts of interest;
Article 16(2), point (d)			
175	(d) the provider shall have appropriate security clearance, at least for personnel intended for service deployment;	(d) the provider shall have appropriate security clearance, at least for personnel intended for service deployment;	(d) the provider shall have appropriate security clearance, at least for personnel intended for service deployment**, where required by a Member State**;
Article 16(2), point (e)			
176	(e) the provider shall have the relevant level of security for its IT systems;	(e) the provider shall have the relevant level of security for its IT systems;	(e) the provider shall have the relevant level of security for its IT systems;
Article 16(2), point (f)			
177	(f) the provider shall be equipped with the hardware and software technical equipment necessary to support the requested service;	(f) the provider shall be equipped with ***up to date*** the hardware and software technical equipment necessary to support the requested service ***and shall, as applicable, comply with Regulation (EU) .../... of the European Parliament and of the Council[1] (2022/0272(COD))***;	(f) the provider shall be equipped with the hardware and software technical equipment necessary to support the requested service;

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
		_____ *1. [1] Regulation (EU) .../... of the European Parliament and of the Council of ... on ... (OJ L, …, ELI: …).*	
Article 16(2), point (g)			
178	(g) the provider shall be able to demonstrate that it has experience in delivering similar services to relevant national authorities or entities operating in critical or highly critical sectors;	(g) the provider shall be able to demonstrate that it has experience in delivering similar services to relevant national authorities or entities operating in critical or highly critical sectors;	(g) the provider shall be able to demonstrate that it has experience in delivering similar services to relevant national authorities or entities operating in ~~critical or highly~~**sectors of high criticality or other** critical sectors;
Article 16(2), point (h)			
179	(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;	(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;	(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;
Article 16(2), point (i)			
180	(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;	(i) the provider shall be able to provide the service in the local language of the Member State(s)*, or in one of the working languages of the Union's institutions,* ~~-~~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(s)**;
Article 16(2), point (j)			
181	(j) once an EU certification scheme for	(j) once an ~~EU~~*European cybersecurity*	(j) once an EU certification scheme for

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
	managed security service Regulation (EU) 2019/881 is in place, the provider shall be certified in accordance with that scheme.	certification scheme for managed security service ***pursuant to*** Regulation (EU) 2019/881 is in place, the provider shall be certified in accordance with that scheme ***within a period of two years after the scheme has been adopted***.	managed security service Regulation (EU) 2019/881 is in place, the provider shall be certified in accordance with that scheme.
Article 16(2), point (ja)			
181a		***(ja) the provider shall be able to provide the service independently and not as part of a bundle, thus safeguarding the user possibility to switch to another service provider;***	
Article 16(2), point (ja)			
181b			**(k) the provider shall include in the tender, the conversion conditions for any unused incident response service that could be converted into preparedness services closely related to incident response, such as exercises or trainings.**
Article 16(2), point (jb)			
181c		***(jb) for the purposes of Article 12(1) the provider shall include in the tenders proposal the possibility for conversion of unused incident response services into exercises or trainings;***	
Article 16(2), point (jc)			

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
181d		***(jc) the provider shall be established and shall have its executive management structures in the Union, in an associated country or in a third country that is part to the Government Procurement Agreement in the context of World Trade Organisation(GPA).***	
Article 16(2), point (jd)			
181e		***(jd) The provider shall not be subject to control by a non-associated third country or by a non-associated third-country entity that is not party to the GPA or, alternatively, such an entity shall have been subject to screening within the meaning of Regulation (EU) 2019/452 and, where necessary, to mitigation measures, taking into account the objectives set out in this Regulation.***	
Article 16(2a)			
181f			**2a. For the purposes of procuring services for the EU Cybersecurity Reserve, the contracting authority shall, where appropriate, develop selection criteria in addition to those referred to in paragraph 2, in close cooperation with Member States.**
Article 16a			
181g			

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
			Article 16a **Mutual assistance**
Article 16a(1)			
181h			**1. The Mechanism shall provide support for technical assistance from one Member State to another Member State affected by a significant or large-scale cybersecurity incident, including in cases referred to in Article 11(3), point (f), of Directive (EU) 2022/2555.**
Article 16a(2)			
181i			**2. The support for the technical mutual assistance referred to in paragraph 1 shall be granted in the form of grants and under the conditions defined in the relevant work programmes referred to in Article 24 of the Digital Europe Programme.**
Article 17			
182	Article 17 Support to third countries	Article 17 Support to third countries	Article 17 Support to **DEP-associated** third countries
Article 17(1)			
183	1. Third countries may request support from	1. Third countries may request support from	1. **A DEP-associated** third ~~countries~~**country**

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
	the EU Cybersecurity Reserve where Association Agreements concluded regarding their participation in DEP provide for this.	the EU Cybersecurity Reserve where Association Agreements concluded regarding their participation in DEP provide for this.	may request support from the EU Cybersecurity Reserve where ~~Association Agreements concluded regarding their participation in DEP provide for this~~**the agreement, through which it is associated to DEP provides for participation in the Reserve**.
Article 17(2)			
184	2. Support from the EU Cybersecurity Reserve shall be in accordance with this Regulation, and shall comply with any specific conditions laid down in the Association Agreements referred to in paragraph 1.	2. Support from the EU Cybersecurity Reserve shall be in accordance with this Regulation, and shall comply with any specific conditions laid down in the Association Agreements referred to in paragraph 1.	2. Support from the EU Cybersecurity Reserve ~~shall be in accordance with this Regulation, and~~**to a DEP-associated third country** shall comply with any specific conditions laid down in the ~~Association Agreements~~ **agreement,** referred to in paragraph 1.
Article 17(3)			
185	3. Users from associated third countries eligible to receive services from the EU Cybersecurity Reserve shall include competent authorities such as CSIRTs and cyber crisis management authorities.	3. Users from associated third countries eligible to receive services from the EU Cybersecurity Reserve shall include competent authorities such as CSIRTs and cyber crisis management authorities.	3. Users from ~~associated~~**DEP-associated** third countries eligible to receive services from the EU Cybersecurity Reserve shall include competent authorities such as **Computer Security Incident and Response Teams** ~~CSIRTs~~ and cyber crisis management authorities.
Article 17(4)			
186	4. Each third country eligible for support from the EU Cybersecurity Reserve shall designate an authority to act as a single point of contact	4. Each third country eligible for support from the EU Cybersecurity Reserve shall designate an authority to act as a single point of contact	4. Each **DEP-associated** third country eligible for support from the EU Cybersecurity Reserve shall designate an authority to act as a single

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
	for the purpose of this Regulation.	for the purpose of this Regulation.	point of contact for the purpose of this Regulation.
Article 17(4a)			
186a			**4a. Requests for support from the EU Cybersecurity Reserve under this Article shall be assessed by the Commission. A response shall be transmitted to the users referred to in Article 12(3) point (c) without undue delay, following the Council's implementing decision referred to in paragraph 5a of this Article.**
Article 17(5)			
187	5. Prior to receiving any support from the EU Cybersecurity Reserve, third countries shall provide to the Commission and the High Representative information about their cyber resilience and risk management capabilities, including at least information on national measures taken to prepare for significant or large-scale cybersecurity incidents, as well as information on responsible national entities, including CSIRTs or equivalent entities, their capabilities and the resources allocated to them. Where provisions of Articles 13 and 14 of this Regulation refer to Member States, they shall apply to third countries as set out in paragraph 1.	5. Prior to receiving any support from the EU Cybersecurity Reserve, third countries shall provide to the Commission and the High Representative information about their cyber resilience and risk management capabilities, including at least information on national measures taken to prepare for significant or large-scale cybersecurity incidents, as well as information on responsible national entities, including CSIRTs or equivalent entities, their capabilities and the resources allocated to them. Where provisions of Articles 13 and 14 of this Regulation refer to Member States, they shall apply to third countries as set out in paragraph 1.	5. **In order to enable the Commission to apply the criteria listed in Article 14(2), within three months of the conclusion of the agreement referred to in paragraph 1 and in any event** prior to receiving any support from the EU cybersecurity reserve, **the DEP-associated** third countries shall provide to the Commission ~~and the High Representative~~ information about their cyber resilience and risk management capabilities, including at least information on national measures taken to prepare for significant**, large-scale or large-scale-equivalent** ~~or large-scale~~ cybersecurity incidents, as well as information on responsible national entities, including CSIRTs or equivalent entities, their capabilities and the

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
			resources allocated to them. ~~Where provisions of Articles 13 and 14 of this Regulation refer to Member States, they shall apply to third countries as set out~~ **The DEP-associated third country shall provide updates to this information on a regular basis and at least once per year. The Commission shall share this information with the High Representative and ENISA for the purpose of facilitating the consultation referred to** in paragraph ~~1~~**6. It shall also share this information with EU CyCLONe**.
Article 17(5a)			
187a			**5a. Support from the EU Cybersecurity Reserve to a DEP-associated third country shall only be provided after a Council implementing decision has been adopted on a proposal from the Commission following its assessment under Article 14 (2). The Council implementing decision authorising the Commission to provide support to the DEP-associated third country shall specify the time period during which such support may be provided, which shall not be longer than three months. It shall be based on an assessment of the support with regard to the criterion for prioritising multiple requests under Article 14(2)(f) of this Regulation and consistency with the Union's policy towards the DEP-associated third country concerned.**

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
Article 17(6)			
188	6. The Commission shall coordinate with the High Representative about the requests received and the implementation of the support granted to third countries from the EU Cybersecurity Reserve.	6. The Commission shall ***without undue delay notify the Council and*** coordinate with the High Representative about the requests received and the implementation of the support granted to third countries from the EU Cybersecurity Reserve.	6. The Commission shall ~~coordinate~~**cooperate** with the High Representative- about the requests received and the implementation of the support granted to **DEP-associated** third countries from the EU Cybersecurity Reserve. **The Commission shall also take into account any views provided by ENISA in respect of those requests.**
Article 17a			
188a			**Article 17a** **Coordination with Union crisis management mechanisms**
Article 17a(1)			
188b			**1. Where a significant cybersecurity incident, a large-scale or large-scale-equivalent cybersecurity incident originates from or results in a disaster as defined in Article 4, point (1), of Decision No 1313/2013/EU, the support provided under this Regulation for responding to such incident shall complement actions under, and be without prejudice, to Decision No 1313/2013/EU.**
Article 17a(2)			

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
188c			**2. In the event of a large-scale or large-scale-equivalent cybersecurity incident where the EU Integrated Political Crisis Response Arrangements under Implementing Decision (EU) 2018/19934 (IPCR Arrangements) are triggered, support provided under this Regulation for responding to such incident shall be handled in accordance with the relevant procedures under the IPCR Arrangements.**
Chapter IV			
189	Chapter IV CYBERSECURITY INCIDENT REVIEW MECHANISM	Chapter IV CYBERSECURITY INCIDENT REVIEW MECHANISM	Chapter IV CYBERSECURITY INCIDENT REVIEW MECHANISM
Article 18			
190	Article 18 Cybersecurity Incident Review Mechanism	Article 18 Cybersecurity Incident Review Mechanism	Article 18 Cybersecurity Incident Review Mechanism
Article 18(1)			
191	1. At the request of the Commission, the EU-CyCLONe or the CSIRTs network, ENISA shall review and assess threats, vulnerabilities and mitigation actions with respect to a specific significant or large-scale cybersecurity incident. Following the completion of a review and	1. At the request of the Commission, the EU-CyCLONe or the CSIRTs network, ENISA shall review and assess threats, vulnerabilities and mitigation actions with respect to a specific significant or large-scale cybersecurity incident. Following the completion of a review and	1. At the request of ~~the Commission, the EU-CyCLONe or~~**, EU-CyCLONe, ENISA shall, with the support of** the CSIRTs network~~,~~ ~~ENISA shall~~ **and with the approval of the Member States concerned,** review and assess threats, **known exploitable** vulnerabilities and

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
	assessment of an incident, ENISA shall deliver an incident review report to the CSIRTs network, the EU-CyCLONe and the Commission to support them in carrying out their tasks, in particular in view of those set out in Articles 15 and 16 of Directive (EU) 2022/2555. Where relevant, the Commission shall share the report with the High Representative.	assessment of an incident, ENISA shall deliver an incident review report to the CSIRTs network, the EU-CyCLONe and the Commission to support them in carrying out their tasks, in particular in view of those set out in Articles 15 and 16 of Directive (EU) 2022/2555. Where relevant, the Commission shall share the report with the High Representative.	mitigation actions with respect to a specific significant or large-scale cybersecurity incident. Following the completion of a review and assessment of an incident, ENISA shall deliver an incident review report **with the aim of drawing lessons-learned to avoid or mitigate future incidents to the EU-CyCLONe,** ~~to~~ the CSIRTs network, **the Member State concerned** ~~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. **When an incident has an impact on a DEP-associated third country** ~~Where relevant~~, **ENISA shall also share the report with the Council.** The Commission shall share the report with the High Representative.
Article 18(2)			
192	2. To prepare the incident review report referred to in paragraph 1, ENISA shall collaborate all relevant stakeholders, including representatives of Member States, the Commission, other relevant EU institutions, bodies and agencies, managed security services providers and users of cybersecurity services. Where appropriate, ENISA shall also collaborate with entities affected by significant or large-scale cybersecurity incidents. To support the review, ENISA may also consult other types of stakeholders. Consulted representatives shall disclose any potential	2. To prepare the incident review report referred to in paragraph 1, ENISA shall collaborate ***with and gather feedback from*** all relevant stakeholders, including representatives of Member States, the Commission, other relevant EU institutions, bodies***, offices*** and agencies, managed security services providers ***in the National and Cross-border SOCs*** and users of cybersecurity services***, complemented with guarantees and monitoring that is adequate to ensure that lessons learned and best practicies identified are backed by the actors in the cybersecurity services industry***.	2. To prepare the incident review report referred to in paragraph 1, ENISA shall collaborate **with** all relevant stakeholders, including representatives of Member States, the Commission, other relevant EU institutions, bodies and agencies, managed security services providers and users of cybersecurity services. Where appropriate, **and with the approval of the Member State(s) concerned,** ENISA shall also collaborate with entities affected by significant or large-scale cybersecurity incidents. ~~To support the review, ENISA may also consult other types of stakeholders.~~

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
	conflict of interest.	Where appropriate, ENISA shall also collaborate with entities affected by significant or large-scale cybersecurity incidents. To support the review, ENISA may also consult other types of stakeholders. Consulted representatives shall disclose any potential conflict of interest.	Consulted representatives shall disclose any potential conflict of interest.
Article 18(3)			
193	3. The report shall cover a review and analysis of the specific significant or large-scale cybersecurity incident, including the main causes, vulnerabilities and lessons learned. It shall protect confidential information, in accordance with Union or national law concerning the protection of sensitive or classified information.	3. The report shall cover a review and analysis of the specific significant or large-scale cybersecurity incident, including the main causes, vulnerabilities and lessons learned. It shall protect confidential information, in accordance with Union or national law concerning the protection of sensitive or classified information. ***It shall not include any details about actively exploited vulnerabilities that remain unpatched.***	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 **information, in particular** ~~confidential information,~~ in accordance with Union or national law concerning the protection of sensitive or classified information. **If the Member State(s) or other user(s) concerned so requests, the report shall contain only anonymised data.**
Article 18(3a)			
193a		***3a. The report referred to in paragraph 1 of this Article shall set out lessons learned from the peer reviews carried out pursuant to Article 19 of Directive (EU) 2022/2555.***	
Article 18(4)			
194			

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
	4. Where appropriate, the report shall draw recommendations to improve the Union's cyber posture.	4. Where appropriate, the report shall draw recommendations***, including for all relevant stakeholders,*** to improve the Union's cyber posture.	4. Where appropriate, the report shall draw recommendations to improve the Union's cyber posture.
Article 18(5)			
195	5. Where possible, a version of the report shall be made available publicly. This version shall only include public information.	5. Where possible, a version of the report shall be made available publicly. This version shall only include public information.	5. ~~Where possible, a version~~**With the approval** of the ~~report shall be made available publicly. This~~**Member State(s) concerned, ENISA may publish a** version ~~shall only include~~**of the report containing only** public information.
Chapter V			
196	Chapter V FINAL PROVISIONS	Chapter V FINAL PROVISIONS	Chapter V FINAL PROVISIONS
Article 19			
197	Article 19 Amendments to Regulation (EU) 2021/694	Article 19 Amendments to Regulation (EU) 2021/694	Article 19 Amendments to Regulation (EU) 2021/694
Article 19, first paragraph			
198	Regulation (EU) 2021/694 is amended as follows:	Regulation (EU) 2021/694 is amended as follows:	Regulation (EU) 2021/694 is amended as follows:
Article 19, first paragraph, point (1)			

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
199	(1) Article 6 is amended as follows:	(1) Article 6 is amended as follows:	(1) Article 6 is amended as follows:
Article 19, first paragraph, point (1)(a)			
200	(a) paragraph 1 is amended as follows:	(a) paragraph 1 is amended as follows:	(a) paragraph 1 is amended as follows:
Article 19, first paragraph, point (1)(a)(1)			
201	(1) the following point (aa) is inserted:	(1) the following point (aa) is inserted:	(1) the following point (aa) is inserted:
Article 19, first paragraph, point (1)(a)(1), amending provision, numbered paragraph (aa)			
202	‘(aa) support the development of an EU Cyber Shield, including the development, deployment and operation of National and Cross-border SOCs platforms that contribute to situational awareness in the Union and to enhancing the cyber threat intelligence capacities of the Union;’	‘(aa) support the development of an EU Cyber Shield, including the development, deployment and operation of National and Cross-border SOCs platforms that contribute to situational awareness in the Union and to enhancing the cyber threat intelligence capacities of the Union;’	‘(aa) support the development of an EU **Cybersecurity Alert System** ~~Cyber Shield~~, including the development, deployment and operation of National **Cyber Hubs and Cross-Border Cyber Hubs** ~~and Cross-border SOCs platforms~~ that contribute to situational awareness in the Union and to enhancing the cyber threat intelligence capacities of the Union;’
Article 19, first paragraph, point (1)(a)(2)			
203	(2) the following point (g) is added:	(2) the following point (g) is added:	(2) the following point (g) is added:
Article 19, first paragraph, point (1)(a)(2), amending provision, numbered paragraph (g)			

www.parlament.gv.at

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate	
	204	‘ (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; ’	‘ (g) establish and operate a ~~Cyber~~***Cybersecurity*** 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; ’	‘ (g) establish and operate a Cyber Emergency Mechanism to support Member States in preparing for and responding to significant cybersecurity incidents, complementary to national resources and capabilities and other forms of support available at Union level, including the establishment of an EU Cybersecurity Reserve **deployable upon request in all Member States, Union institutions, bodies and agencies and in certain third countries**; ’	
Article 19, first paragraph, point (1)(b)				
G	205	(b) Paragraph 2 is replaced by the following:	(b) Paragraph 2 is replaced by the following:	(b) Paragraph 2 is replaced by the following:	G
Article 19, first paragraph, point (1)(b), amending provision, numbered paragraph (2)				
G	206	‘ 2. The actions under Specific Objective 3 shall be implemented primarily through the European Cybersecurity Industrial, technology and research Competence Centre and the Network of National Coordination Centres, in accordance with Regulation (EU) 2021/887 of the European Parliament and of the Council[1] with the exception of actions implementing the EU Cybersecurity Reserve, which shall be implemented by the Commission and ENISA.';	‘ 2. The actions under Specific Objective 3 shall be implemented primarily through the European Cybersecurity Industrial, technology and research Competence Centre and the Network of National Coordination Centres, in accordance with Regulation (EU) 2021/887 of the European Parliament and of the Council[1] with the exception of actions implementing the EU Cybersecurity Reserve, which shall be implemented by the Commission and ENISA.';	‘ 2. The actions under Specific Objective 3 shall be implemented primarily through the European Cybersecurity Industrial, technology and research Competence Centre and the Network of National Coordination Centres, in accordance with Regulation (EU) 2021/887 of the European Parliament and of the Council[1] with the exception of actions implementing the EU Cybersecurity Reserve, which shall be implemented by the Commission and ENISA.';	G

	Commission Proposal	EP Mandate	Council Mandate
	' __________ 1. Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, (OJ L 202, 8.6.2021, p. 1-31).	' __________ 1. Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, (OJ L 202, 8.6.2021, p. 1-31).	' __________ 1. Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, (OJ L 202, 8.6.2021, p. 1-31).
Article 19, first paragraph, point (2)			
G 207	(2) Article 9 is amended as follows:	(2) Article 9 is amended as follows:	(2) Article 9 is amended as follows: G
Article 19, first paragraph, point (2)(a)			
G 208	(a) in paragraph 2, points (b), (c) and (d) are replaced by the following:	(a) in paragraph 2, points (b), (c) and (d) are replaced by the following:	(a) in paragraph 2, points (b), (c) and (d) are replaced by the following: G
Article 19, first paragraph, point (2)(a), amending provision, numbered paragraph (b)			
G 209	' (b) , EUR 1 776 956 000 for Specific Objective 2 – Artificial Intelligence;	' (b) , EUR 1 776 956 000 for Specific Objective 2 – Artificial Intelligence;	' (b) , EUR 1 776 956 000 for Specific Objective 2 – Artificial Intelligence; G
Article 19, first paragraph, point (2)(a), amending provision, numbered paragraph (c)			
210	(c) , EUR 1 629 566 000 for Specific Objective 3 – Cybersecurity and Trust;	(c) ~~, EUR 1 629 566 000~~***EUR 1 620 566 000*** for Specific Objective 3 – Cybersecurity and Trust;	(c) , EUR 1 629 566 000 for Specific Objective 3 – Cybersecurity and Trust;
Article 19, first paragraph, point (2)(a), amending provision, numbered paragraph (d)			

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
211	(d) , EUR 482 347 000 for Specific Objective 4 – Advanced Digital Skills; ,	(d) ~~, EUR 482 347 000~~***EUR 500 347 000*** for Specific Objective 4 – Advanced Digital Skills***'***; ,	(d) , EUR 482 347 000 for Specific Objective 4 – Advanced Digital Skills; ,
Article 19, first paragraph, point (2)(aa)			
211a		***(aa) the following new paragraph 2a is inserted:***	
Article 19, first paragraph, point (2)(aa), amending provision, first paragraph			
211b		‘ ***(2a) ‘ The amount referred to in paragraph 2 point c shall primarily be used for achieving the operational objectives referred into art. 6 par. 1 (a-f) of the Programme.’;*** ,	
Article 19, first paragraph, point (2)(ab)			
211c		***(ab) the following new paragraph 2b is inserted:***	
Article 19, first paragraph, point (2)(ab), amending provision, first paragraph			
211d		‘ ***(2b) The amount for the establishment and implementation of the EU Cybersecurity Reserve shall not exceed EUR 27 million for***	

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
		the intended duration of the Regulation laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for, and respond to cybersecurity threats and incidents.';	
Article 19, first paragraph, point (2)(b)			
212	(b) the following paragraph 8 is added:	(b) the following paragraph 8 is added:	(b) the following paragraph 8 is added:
Article 19, first paragraph, point (2)(b), amending provision, numbered paragraph (8)			
213	‘ 8. By derogation to Article 12(4) of Regulation (EU, Euratom) 2018/1046, unused commitment and payment appropriations for actions pursuing the objectives set out in Article 6(1), point (g) of this Regulation, shall be automatically carried over and may be committed and paid up to 31 December of the following financial year.;	‘ 8. By ***way of*** derogation ~~to~~***from*** Article 12(4) of Regulation (EU, Euratom) 2018/1046, unused commitment and payment appropriations for actions ***in the context of the implementation of the EU cybersecurity Reserve,*** pursuing the objectives set out in Article 6(1), point (g) of this Regulation, shall be automatically carried over and may be committed and paid up to 31 December of the following financial year.***'***; ***The Commission shall inform the Parliament and the Council of appropriations carried over in accordance with art. 12(6) of Regulation (EU, Euratom) 2018/1046.***	‘ 8. By ~~derogation to~~ **way of derogation from** Article ~~12(4)~~**12(1** of Regulation (EU, Euratom) 2018/1046, unused commitment and payment appropriations for actions pursuing the objectives set out in Article 6(1), point (g) of this Regulation, shall be automatically carried over and may be committed and paid up to 31 December of the following financial year.;
Article 19, first paragraph, point (2a)			

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
213a			**(2a) Article 12 is amended as follows:**
Article 19, first paragraph, point (2a)(a), first subparagraph			
213b			**(1) paragraph 5 is replaced by the following:**
Article 19, first paragraph, point (2a)(a), first subparagraph, amending provision, first paragraph			
213c			‘**'5 The work programme may also provide that legal entities established in associated countries and legal entities that are established in the Union but are controlled from third countries are not eligible to participate in all or some actions under Specific Objective 3, for duly justified security reasons. In such cases, calls for proposals and calls for tenders shall be restricted to legal entities established or deemed to be established in Member States and controlled by Member States or by nationals of Member States'.**’
Article 19, first paragraph, point (2a)(a), second subparagraph			
213d			**The first subparagraph of this paragraph shall not apply, insofar as concerns legal entities that are established in the Union but are controlled from third countries, to any**

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
			action implementing the European Cybersecurity Alert System where both of the following conditions are fulfilled in respect of that action:
Article 19, first paragraph, point (2a)(a), second subparagraph, amending provision, first paragraph			
213e			‘ **(a) there is a real risk, taking into account the results of the mapping referred to in Article 8 (3a) of Regulation [Cybersolidarity Act], that the tools, infrastructures and services necessary and sufficient for that action to adequately contribute to the objective of the European Cybersecurity Alert System will not be available from legal entities established or deemed to be established in Member States and controlled by Member States or by nationals of Member States; and**
Article 19, first paragraph, point (2a)(a), second subparagraph, amending provision, second paragraph			
213f			**(b) the security risk of procuring from such legal entities within the European Cybersecurity Alert System is proportionate to the benefits and does not undermine the essential security interests of the Union and its Member States.** ’

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
Article 19, first paragraph, point (2a)(a), third subparagraph			
213g			**The first subparagraph of this paragraph shall not apply, insofar as concerns legal entities that are established in the Union but are controlled from third countries, to actions implementing the EU Cybersecurity Reserve where both of the following conditions are fulfilled:**
Article 19, first paragraph, point (2a)(a), third subparagraph, amending provision, first paragraph			
213h			‘ **(a) there is a real risk, taking into account the results of the mapping referred to in Article 12 (7) of Regulation [Cybersolidarity Act], that the technology, expertise or capacity necessary and sufficient for the EU Cybersecurity Reserve to adequately perform its functions will not be available from legal entities established or deemed to be established in Member States and controlled by Member States or by nationals of Member States; and**
Article 19, first paragraph, point (2a)(a), third subparagraph, amending provision, second paragraph			
213i			**(b) the security risk of including such legal entities within the EU Cybersecurity Reserve is proportionate to the benefits and does not undermine the essential security interests of**

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
			the Union and its Member States.' ’
Article 19, first paragraph, point (2b), first subparagraph			
213j			**(2) paragraph 6 is replaced by the following:**
Article 19, first paragraph, point (2b), first subparagraph, amending provision, first paragraph			
213k			‘ **'6. If duly justified for security reasons, the work programme may also provide that legal entities established in associated countries and legal entities that are established in the Union but are controlled from third countries may be eligible to participate in all or some actions under Specific Objectives 1 and 2, only if they comply with the requirements to be fulfilled by those legal entities to guarantee the protection of the essential security interests of the Union and the Member States and to ensure the protection of classified documents information. Those requirements shall be set out in the work programme.'** ’
Article 19, first paragraph, point (2b), second subparagraph			
213l			**The first subparagraph of this paragraph shall also apply, insofar as concerns legal**

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
			entities that are established in the Union but are controlled from third countries, to actions under Specific Objective 3:
Article 19, first paragraph, point (2b), second subparagraph, amending provision, first paragraph			
213m			‘ **(a) to implement the European Cybersecurity Alert System in cases where paragraph 5, second subparagraph of this Article applies; and**
Article 19, first paragraph, point (2b), second subparagraph, amending provision, second paragraph			
213n			**(b) to implement the EU Cybersecurity Reserve in cases where paragraph 5, third subparagraph of this Article applies.’** ’
Article 19, first paragraph, point (3)			
G 214	(3) In Article 14, paragraph 2 is replaced by the following:	(3) In Article 14, paragraph 2 is replaced by the following:	(3) In Article 14, paragraph 2 is replaced by the following: G
Article 19, first paragraph, point (3), amending provision, numbered paragraph (2), first subparagraph			
215	“ 2. The Programme may provide funding in any of the forms laid down in the Financial Regulation, including in particular through	“ 2. The Programme may provide funding in any of the forms laid down in the ~~*Financial*~~ Regulation ***(EU, Euratom) 2018/1046***,	“ 2. The Programme may provide funding in any of the forms laid down in the Financial Regulation, including in particular through

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
	procurement as a primary form, or grants and prizes.	including in particular through procurement as a primary form, or grants and prizes.	procurement as a primary form, or grants and prizes.
Article 19, first paragraph, point (3), amending provision, numbered paragraph (2), second subparagraph			
G 216	Where the achievement of the objective of an action requires the procurement of innovative goods and services, grants may be awarded only to beneficiaries that are contracting authorities or contracting entities as defined in Directives 2014/24/EU [27] and 2014/25/EU [28] of the European Parliament and of the Council.	Where the achievement of the objective of an action requires the procurement of innovative goods and services, grants may be awarded only to beneficiaries that are contracting authorities or contracting entities as defined in Directives 2014/24/EU [27] and 2014/25/EU [28] of the European Parliament and of the Council.	Where the achievement of the objective of an action requires the procurement of innovative goods and services, grants may be awarded only to beneficiaries that are contracting authorities or contracting entities as defined in Directives 2014/24/EU [27] and 2014/25/EU [28] of the European Parliament and of the Council. G
Article 19, first paragraph, point (3), amending provision, numbered paragraph (2), third subparagraph			
G 217	Where the supply of innovative goods or services that are not yet available on a large-scale commercial basis is necessary to achieve the objectives of an action, the contracting authority or the contracting entity may authorise the award of multiple contracts within the same procurement procedure.	Where the supply of innovative goods or services that are not yet available on a large-scale commercial basis is necessary to achieve the objectives of an action, the contracting authority or the contracting entity may authorise the award of multiple contracts within the same procurement procedure.	Where the supply of innovative goods or services that are not yet available on a large-scale commercial basis is necessary to achieve the objectives of an action, the contracting authority or the contracting entity may authorise the award of multiple contracts within the same procurement procedure. G
Article 19, first paragraph, point (3), amending provision, numbered paragraph (2), fourth subparagraph			
G 218	For duly justified reasons of public security, the contracting authority or the contracting entity may require that the place of performance of the contract be situated within the territory of the Union.	For duly justified reasons of public security, the contracting authority or the contracting entity may require that the place of performance of the contract be situated within the territory of the Union.	For duly justified reasons of public security, the contracting authority or the contracting entity may require that the place of performance of the contract be situated within the territory of the Union. G

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
Article 19, first paragraph, point (3), amending provision, numbered paragraph (2), fifth subparagraph			
G 219	When implementing procurement procedures for the EU Cybersecurity Reserve established by Article 12 of Regulation (EU) 2023/XX, the Commission and ENISA may act as a central purchasing body to procure on behalf of or in the name of third countries associated to the Programme in line with Article 10. The Commission and ENISA may also act as wholesaler, by buying, stocking and reselling or donating supplies and services, including rentals, to those third countries. By derogation from Article 169(3) of Regulation (EU). XXX/XXXX [FR Recast], the request from a single third country is sufficient to mandate the Commission or ENISA to act.	When implementing procurement procedures for the EU Cybersecurity Reserve established by Article 12 of Regulation (EU) 2023/XX, the Commission and ENISA may act as a central purchasing body to procure on behalf of or in the name of third countries associated to the Programme in line with Article 10. The Commission and ENISA may also act as wholesaler, by buying, stocking and reselling or donating supplies and services, including rentals, to those third countries. By derogation from Article 169(3) of Regulation (EU). XXX/XXXX [FR Recast], the request from a single third country is sufficient to mandate the Commission or ENISA to act.	When implementing procurement procedures for the EU Cybersecurity Reserve established by Article 12 of Regulation (EU) 2023/XX, the Commission and ENISA may act as a central purchasing body to procure on behalf of or in the name of third countries associated to the Programme in line with Article 10. The Commission and ENISA may also act as wholesaler, by buying, stocking and reselling or donating supplies and services, including rentals, to those third countries. By derogation from Article 169(3) of Regulation (EU). XXX/XXXX [FR Recast], the request from a single third country is sufficient to mandate the Commission or ENISA to act. G
Article 19, first paragraph, point (3), amending provision, numbered paragraph (2), sixth subparagraph			
G 220	When implementing procurement procedures for the EU Cybersecurity Reserve established by Article 12 of Regulation (EU) 2023/XX, the Commission and ENISA may act as a central purchasing body to procure on behalf of or in the name of Union institutions, bodies and agencies. The Commission and ENISA may also act as wholesaler, by buying, stocking and reselling or donating supplies and services, including rentals, to Union institutions, bodies and agencies. By derogation from Article 169(3) of Regulation (EU) XXX/XXXX [FR	When implementing procurement procedures for the EU Cybersecurity Reserve established by Article 12 of Regulation (EU) 2023/XX, the Commission and ENISA may act as a central purchasing body to procure on behalf of or in the name of Union institutions, bodies and agencies. The Commission and ENISA may also act as wholesaler, by buying, stocking and reselling or donating supplies and services, including rentals, to Union institutions, bodies and agencies. By derogation from Article 169(3) of Regulation (EU) XXX/XXXX [FR	When implementing procurement procedures for the EU Cybersecurity Reserve established by Article 12 of Regulation (EU) 2023/XX, the Commission and ENISA may act as a central purchasing body to procure on behalf of or in the name of Union institutions, bodies and agencies. The Commission and ENISA may also act as wholesaler, by buying, stocking and reselling or donating supplies and services, including rentals, to Union institutions, bodies and agencies. By derogation from Article 169(3) of Regulation (EU) XXX/XXXX [FR G

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
	Recast], the request from a single Union institution, body or agency is sufficient to mandate the Commission or ENISA to act.	Recast], the request from a single Union institution, body or agency is sufficient to mandate the Commission or ENISA to act.	Recast], the request from a single Union institution, body or agency is sufficient to mandate the Commission or ENISA to act.
Article 19, first paragraph, point (3), amending provision, numbered paragraph (2), seventh subparagraph			
221	The Programme may also provide financing in the form of financial instruments within blending operations. ”	The Programme may also provide financing in the form of financial instruments within blending operations. ”	The Programme may also provide financing in the form of financial instruments within blending operations. ”
Article 19, first paragraph, point (4)			
222	(4) The following article 16a is added:	(4) The following article 16a is added:	(4) The following article 16a is added:
Article 19, first paragraph, point (4a)			
222a			
Article 19, first paragraph, point (4), amending provision, first subparagraph -a			
222b		‘ ***Article 16a***	
Article 19, first paragraph, point (4), amending provision, first subparagraph			
223	‘ In the case of actions implementing the European Cyber Shield established by Article 3	In the case of actions implementing the European Cyber Shield established by Article 3 of Regulation (EU) 2023/XX, the applicable	‘ In the case of actions implementing the European **Cybersecurity Alert System** ~~Cyber~~

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
	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. '	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. '	~~Shield~~ established by Article 3 of Regulation (EU) 2023/XX, the applicable rules shall be those set out in Articles 4 and 5 of Regulation (EU) 2023/XX. In the case of conflict between the provisions of this Regulation and Articles 4 and 5 of Regulation (EU) 2023/XX, the latter shall prevail and apply to those specific actions. '
Article 19, first paragraph, point (5)			
224	(5) Article 19 is replaced by the following:	(5) Article 19 is replaced by the following:	(5) Article 19 is replaced by the following:
Article 19, first paragraph, point (5), amending provision, first paragraph			
225	‘ 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.	‘ Grants under the Programme shall be awarded and managed in accordance with Title VIII of ~~*the Financial Regulation*~~***Regulation (EU, Euratom) 2018/1046*** 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*~~***Regulation (EU, Euratom) 2018/1046***. Such grants shall be awarded and managed as specified for each specific objective.	‘ **‘**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.
Article 19, first paragraph, point (5), amending provision, second paragraph			
226	Support in the form of grants may be awarded directly by the ECCC without a call for	Support in the form of grants may be awarded directly by the ECCC without a call for	Support in the form of grants may be awarded directly by the ECCC without a call for

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
	proposals to the National SOCs referred to in Article 4 of Regulation XXXX and the Hosting Consortium referred to in Article 5 of Regulation XXXX, in accordance with Article 195(1), point (d) of the Financial Regulation.	proposals to the National SOCs referred to in Article 4 of Regulation ~~*XXXX*~~***(EU) .../...*** and the Hosting Consortium referred to in Article 5 of Regulation ~~*XXXX*~~***(EU) .../...***, in accordance with Article 195(1), point (d) of ~~*the Financial Regulation*~~***Regulation (EU, Euratom) 2018/1046***.	proposals to the **selected Member States** ~~National SOCs~~ referred to in Article 4 of Regulation XXXX and the Hosting Consortium referred to in Article 5 of Regulation XXXX, in accordance with **[**Article 195(1), point (d) of the Financial Regulation**]**.
Article 19, first paragraph, point (5), amending provision, third paragraph			
227	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.	Support in the form of grants for the ~~*Cyber*~~***Cybersecurity*** Emergency Mechanism as set out in Article 10 of Regulation ~~*XXXX*~~ ***(EU) .../...***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*~~***Regulation (EU, Euratom) 2018/1046***.	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**]**.
Article 19, first paragraph, point (5), amending provision, fourth paragraph			
228	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 actions specified in Article 10(1), point (c) of Regulation ~~*202X/XXXX*~~***(EU) .../...***, the ECCC shall inform the Commission and ENISA about Member States' requests for direct grants without a call for proposals.	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.
Article 19, first paragraph, point (5), amending provision, fifth paragraph			
229	For the support of mutual assistance for response to a significant or large-scale	For the support of mutual assistance for response to a significant or large-scale	For the support of mutual assistance for response to a significant or large-scale

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
	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.; ”	cybersecurity incident as defined in Article 10(c), of Regulation ~~*XXXX*~~***(EU) .../...***, and in accordance with Article 193(2), second subparagraph, point (a), of ~~*the Financial Regulation*~~***Regulation (EU, Euratom) 2018/1046***, in duly justified cases, the costs may be considered to be eligible even if they were~~–~~ incurred before the grant application was submitted.***”***; ”	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.; ”
Article 19, first paragraph, point (6)			
230	(6) Annexes I and II are amended in accordance with the Annex to this Regulation.	(6) Annexes I and II are amended in accordance with the Annex to this Regulation.	(6) Annexes I and II are amended in accordance with the Annex to this Regulation.
Article 19a			
230a		***Article 19a*** ***Additional ressources for ENISA***	
Article 19a, first paragraph			
230b		***ENISA shall receive additional resources to carry out its additional tasks conferred on it by this Regulation. That additional support, including funding, shall not jeopardise the achievement of the objectives of other Union's Programmes, in particular the Digital Europe Programme.***	

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
Article 20			
231	Article 20 Evaluation	Article 20 Evaluation ***and Review***	Article 20 Evaluation
Article 20, first paragraph			
232	By [four years after the date of application of this Regulation], the Commission shall submit a report on the evaluation and review of this Regulation to the European Parliament and to the Council.	***1.*** By [~~*four*~~***two*** years ~~*after*~~***from*** the date of application of this Regulation] ***and every two years thereafter***, the Commission shall ~~*submit a report on the evaluation and review of*~~***carry out an evaluation of the functioning of the measures laid down in*** this Regulation ***and shall submit a report*** to the European Parliament and to the Council.	By [four years after the date of application of this Regulation], the Commission shall submit a report on the evaluation and review of this Regulation to the European Parliament and to the Council. **The report shall in particular assess the effectiveness of the European Cyber Security Alert System, the Cyber Emergency Mechanism and the use of funding from DEP. It shall also assess how the regulation has contributed to reinforcing solidarity and the competitive position of industry and services sectors in the Union across the digital economy as well as to the Union's technological sovereignty in the area of cybersecurity.**
Article 20, first paragraph a			
232a		***2. The evaluation shall assess in particular:***	
Article 20, first paragraph a, point (a)			
232b			

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
		(a) the use and added value of the Cross-Border SOCs and the extent to which they contribute to fastering the detection of and respone to cyber threats and situational awareness; the active participation of National SOCs in the European Cyber Shield, including the number of National SOCs and Cross-border SOCs established and the extent to which it has contributed to the production and exchange of high-quality actionable information and cyber threat intelligence; the number and costs of cybersecurity infrastructure, or tools, or both jointly procured; the number of cooperation agreements concluded between Cross-border SOCs and with industry ISACs; the number of incidents reported to the CSIRT network and the impact it has on the work of the CSIRT Network;	
Article 20, first paragraph a, point (b)			
232c		***(b) both the positive and the negative working of the Cybersecurity Emergency Mechanism, including whether further cooperation or training requirements are needed;***	
Article 20, first paragraph a, point (c)			
232d		***(c) the contribution of this Regulation to reinforce the Union's resilience and open strategic autonomy, to improve the***	

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
		competitiveness of the relevant industry sectors, microenterprises, SMEs including start-ups, and the development of cybersecurity skills in the Union;	
Article 20, first paragraph a, point (d)			
232e		***(d) the use and added value of the EU Cybersecurity Reserve, including the number of trusted security providers part of the EU Cybersecurity Reserve; the number, type, costs and impact of actions carried out supporting response to cybersecurity incidents, as well as its users and providers; the mean time for the Commission to acknowledge, the EU Cybersecurity Reserve to be deployed and to respond, and the user to recover from incidents; whether the scope of the EU Cybersecurity Reserve is to be broadened to incident preparedness services or common exercises with the trusted managed securiy service providers and potential users of the EU Cybersecurity Reserve to ensure efficient functioning of the EU Cybersecurity Reserve where necessary;***	
Article 20, first paragraph a, point (e)			
232f		***(e) the contribution of this Regulation to the development and improvement of the skills and competences of the workforce in the cybersecurity sector, needed to strengthen the***	

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
		Union's capacity to detect, prevent, respond to and recover from cybersecurity threats and incidents;	
Article 20, first paragraph a, point (f)			
232g		***(f) the contribution of this Regulation to the deployment and development of state-of-the-art technologies in the Union.***	
Article 20, third paragraph			
232h		***3. On the basis of the reports referred to in paragraph 1, the Commission shall, where appropriate, submit a legislative proposal to the European Parliament and to the Council to amend this Regulation.***	
Article 20a			
232i		***Article 20a*** ***Exercise of the delegation***	
Article 20a(1)			
232j		***1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.***	
Article 20a(2)			

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
232k		***2. The power to adopt delegated acts referred to in Article 6(3), Article 7(2), Article 12(8) and Article 13(7) shall be conferred on the Commission for a period of … years from … [date of entry into force of the basic legislative act or any other date set by the co-legislators]. The Commission shall draw up a report in respect of the delegation of power not later than nine months before the end of the … year period. The delegation of power shall be tacitly extended for periods of an identical duration, unless the European Parliament or the Council opposes such extension not later than three months before the end of each period.***	
Article 20a(3)			
232l		***3. The delegation of power referred to in Article 6(3), Article 7(2), Article 12(8) and Article 13(7) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.***	
Article 20a(4)			
232m			

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
		4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making.	
Article 20a(5)			
232n		***5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.***	
Article 20a(6)			
232o		***6. A delegated act adopted pursuant to Article 6(3), Article 7(2), Article 12(8) or Article 13(7) shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by [two months] at the initiative of the European Parliament or of the Council.***	
Article 21			
233			

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
	Article 21 Committee procedure	Article 21 Committee procedure	Article 21 Committee procedure
Article 21(1)			
234	1. The Commission shall be assisted by the Digital Europe Programme Coordination Committee established by Regulation (EU) 2021/694. That committee shall be a committee within the meaning of Regulation (EU) 182/2011.	1. The Commission shall be assisted by the Digital Europe Programme Coordination Committee established by Regulation (EU) 2021/694. That committee shall be a committee within the meaning of Regulation (EU) 182/2011.	1. The Commission shall be assisted by the Digital Europe Programme Coordination Committee established by Regulation (EU) 2021/694. That committee shall be a committee within the meaning of Regulation (EU) 182/2011.
Article 21(2)			
235	2. Where reference is made to this paragraph, Article 5 of Regulation (EU) 182/2011 shall apply.	2. Where reference is made to this paragraph, Article 5 of Regulation (EU) 182/2011 shall apply.	2. Where reference is made to this paragraph, Article 5 of Regulation (EU) 182/2011 shall apply.
Article 22			
236	Article 22 Entry into force	Article 22 Entry into force	Article 22 Entry into force
Article 22, first paragraph			
237	This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.	This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.	This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.
Article 22, second paragraph			

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate	
G 238	This Regulation shall be binding in its entirety and directly applicable in all Member States.	This Regulation shall be binding in its entirety and directly applicable in all Member States.	This Regulation shall be binding in its entirety and directly applicable in all Member States.	G
Formula				
G 239	Done at Strasbourg,	Done at Strasbourg,	Done at Strasbourg,	G
Formula				
G 240	For the European Parliament	For the European Parliament	For the European Parliament	G
Formula				
G 241	The President	The President	The President	G
Formula				
G 242	For the Council	For the Council	For the Council	G
Formula				
G 243	The President	The President	The President	G
Annex				
244	Annex	Annex	Annex	

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
Annex, first paragraph			
245	Regulation (EU) 2021/694 is amended as follows:	Regulation (EU) 2021/694 is amended as follows:	Regulation (EU) 2021/694 is amended as follows:
Annex, second paragraph			
246	(1) In Annex I, the section/ chapter 'Specific Objective 3 – Cybersecurity and Trust' is replaced by the following:	(1) In Annex I, the section/ chapter 'Specific Objective 3 – Cybersecurity and Trust' is replaced by the following:	(1) In Annex I, the section/ chapter 'Specific Objective 3 – Cybersecurity and Trust' is replaced by the following:
Annex, second paragraph, amending provision, first paragraph			
247	' Specific Objective 3 – Cybersecurity and Trust	' Specific Objective 3 – Cybersecurity and Trust	' Specific Objective 3 – Cybersecurity and Trust
Annex, second paragraph, amending provision, second paragraph			
248	The Programme shall stimulate the reinforcement, building and acquisition of essential capacities to secure the Union's digital economy, society and democracy by reinforcing the Union cybersecurity industrial potential and competitiveness, as well as by improving capabilities of both the private and public sectors to protect citizens and businesses from cyber threats, including by supporting the implementation of Directive (EU) 2016/1148.	The Programme shall stimulate the reinforcement, building and acquisition of essential capacities to secure the Union's digital economy, society and democracy by reinforcing the Union cybersecurity industrial potential and competitiveness, as well as by improving capabilities of both the private and public sectors to protect citizens and businesses from cyber threats, including by supporting the implementation of Directive (EU) 2016/1148.	The Programme shall stimulate the reinforcement, building and acquisition of essential capacities to secure the Union's digital economy, society and democracy by reinforcing the Union cybersecurity industrial potential and competitiveness, as well as by improving capabilities of both the private and public sectors to protect citizens and businesses from cyber threats, including by supporting the implementation of Directive (EU) 2016/1148.
Annex, second paragraph, amending provision, third paragraph			

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
249	Initial and, where appropriate, subsequent actions under this objective shall include:	Initial and, where appropriate, subsequent actions under this objective shall include:	Initial and, where appropriate, subsequent actions under this objective shall include:
Annex, second paragraph, amending provision, third paragraph, point (1)			
250	1. Co-investment with Member States in advanced cybersecurity equipment, infrastructures and knowhow that are essential to protect critical infrastructures and the Digital Single Market at large. Such co-investment could include investments in quantum facilities and data resources for cybersecurity, situational awareness in cyberspace including National SOCs and Cross-border SOCs forming the European Cyber Shield, as well as other tools to be made available to public and private sector across Europe.	1. Co-investment with Member States in advanced cybersecurity equipment, infrastructures and knowhow that are essential to protect critical infrastructures and the Digital Single Market at large. Such co-investment could include investments in quantum facilities and data resources for cybersecurity, situational awareness in cyberspace including National SOCs and Cross-border SOCs forming the European Cyber Shield, as well as other tools to be made available to public and private sector across Europe.	1. Co-investment with Member States in advanced cybersecurity equipment, infrastructures and knowhow that are essential to protect critical infrastructures and the Digital Single Market at large. Such co-investment could include investments in quantum facilities and data resources for cybersecurity, situational awareness in cyberspace -including National ~~SOCs~~ **Cyber Hubs** and Cross-border ~~SOCs~~**Cyber Hubs** forming the European ***Cyber* Alert System** ~~Cyber Shield~~, as well as other tools to be made available to public and private sector across Europe.
Annex, second paragraph, amending provision, third paragraph, point (2)			
251	2. Scaling up existing technological capacities and networking the competence centres in Member States and making sure that those capacities respond to public sector and industry needs, including through products and services that reinforce cybersecurity and trust within the Digital Single Market.	2. Scaling up existing technological capacities and networking the competence centres in Member States and making sure that those capacities respond to public sector and industry needs, including through products and services that reinforce cybersecurity and trust within the Digital Single Market.	2. Scaling up existing technological capacities and networking the competence centres in Member States and making sure that those capacities respond to public sector and industry needs, including through products and services that reinforce cybersecurity and trust within the Digital Single Market.
Annex, second paragraph, amending provision, third paragraph, point (3)			

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
252	3. Ensuring wide deployment of effective state-of-the-art cybersecurity and trust solutions across the Member States. Such deployment includes strengthening the security and safety of products, from their design to their commercialisation.	3. Ensuring wide deployment of effective state-of-the-art cybersecurity and trust solutions across the Member States. Such deployment includes strengthening the security and safety of products, from their design to their commercialisation.	3. Ensuring wide deployment of effective state-of-the-art cybersecurity and trust solutions across the Member States. Such deployment includes strengthening the security and safety of products, from their design to their commercialisation.
Annex, second paragraph, amending provision, third paragraph, point (4)			
253	4. Support closing the cybersecurity skills gap by, for example, aligning cybersecurity skills programmes, adapting them to specific sectorial needs and facilitating access to targeted specialised training.	4. Support closing the cybersecurity skills gap***, with a particular focus on achieving gender balance in the sector*** by, for example, aligning cybersecurity skills programmes, adapting them to specific sectorial needs***, including an interdisciplinary and general focus*** and facilitating access to targeted specialised training ***to enable all persons and territories, without prejudice to the possibility of benefiting from the opportunities provided by this Regulation***.	4. Support closing the cybersecurity skills gap by, for example, aligning cybersecurity skills programmes, adapting them to specific sectorial needs and facilitating access to targeted specialised training.
Annex, second paragraph, amending provision, third paragraph, point (5)			
254	5. Promoting solidarity among Member States in preparing for and responding to significant cybersecurity incidents through deployment of cybersecurity services across borders, including support for mutual assistance between public authorities and the establishment of a reserve of trusted cybersecurity providers at Union level.; ’	5. Promoting solidarity among Member States in preparing for and responding to significant cybersecurity incidents through deployment of cybersecurity services across borders, including support for mutual assistance between public authorities and the establishment of a reserve of trusted ~~*cybersecurity*~~***managed security service*** providers- at Union level.’;	5. Promoting solidarity among Member States in preparing for and responding to significant cybersecurity incidents through deployment of cybersecurity services across borders, including support for mutual assistance between public authorities and the establishment of a reserve of trusted cybersecurity providers at Union level.; ’

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
		’	
Annex, third paragraph			
255	(2) In Annex II the section/chapter ‘Specific Objective 3 – Cybersecurity and Trust’ is replaced by the following:	(2) In Annex II the section/chapter ‘Specific Objective 3 – Cybersecurity and Trust’ is replaced by the following:	(2) In Annex II the section/chapter ‘Specific Objective 3 – Cybersecurity and Trust’ is replaced by the following:
Annex, third paragraph, amending provision, first paragraph			
256	‘ Specific Objective 3 – Cybersecurity and Trust	‘ Specific Objective 3 – Cybersecurity and Trust	‘ Specific Objective 3 – Cybersecurity and Trust
Annex, third paragraph, amending provision, numbered paragraph (3.1)			
257	3.1. The number of cybersecurity infrastructure, or tools, or both jointly procured	3.1. The number of cybersecurity infrastructure, or tools, or both jointly procured ***as part of the Cybersecurity Shield.***	3.1. The number of cybersecurity infrastructure, or tools, or both jointly procured
Annex, third paragraph, amending provision, numbered paragraph (3.2)			
258	3.2. The number of users and user communities getting access to European cybersecurity facilities	3.2. The number of users and user communities getting access to European cybersecurity facilities	3.2. The number of users and user communities getting access to European cybersecurity facilities
Annex, third paragraph, amending provision, numbered paragraph (3.3)			
259	3.3 The number of actions supporting preparedness and response to cybersecurity	3.3 The number***, type, costs and impact*** of actions ***carried out*** supporting preparedness and	3.3 The number of actions supporting preparedness and response to cybersecurity

www.parlament.gv.at

	Commission Proposal	EP Mandate	Council Mandate
	incidents under the Cyber Emergency Mechanism. ,	response to cybersecurity incidents under the ~~*Cyber*~~***Cybersecurity*** Emergency Mechanism. ***The extent to which recommendations of preparedness tests have been implemented and carried out by the user as well as the mean time for the Commission to acknowledge, the EU Cybersecurity Reserve to respond, and the user to recover from incidents.'*** ,	incidents under the Cyber Emergency Mechanism. ,
Annex …			
260	Annex […]	Annex […]	Annex […]

www.parlament.gv.at