European Parliament
2019-2024

Committee on Constitutional Affairs

2022/0085(COD)

31.1.2023

OPINION

of the Committee on Constitutional Affairs

for the Committee on Industry, Research and Energy

on the proposal for a regulation of the European Parliament and of the Council laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union
(COM(2022)0122 – C9-0122/2022 – 2022/0085(COD))

Rapporteur for opinion: Markéta Gregorová

PA_Legam

SHORT JUSTIFICATION

European Union institutions, bodies and agencies operate in recent years against an increasingly digitalised background of constant technological developments and of ensuing evolving cybersecurity threat levels. This situation has been exacerbated by the onset of the COVID-19 sanitary crisis and inter alia, the increased teleworking practices, during which the number of sophisticated attacks coming from a wide range of sources continued to rise.

Currently, the cybersecurity landscape, including the governance, cyber-hygiene, overall capability and maturity, differs considerably among Union institutions, bodies and agencies, which creates a further obstacle to an open, efficient and independent European administration.

Therefore, the rapporteur agrees that a baseline approach among Union institutions, bodies and agencies for the establishment of common systems and requirements of cybersecurity would be necessary to ensure that cybersecurity develops in the same direction, thus contributing to the efficiency and the independence of the European administration.

The rapporteur further believes that a robust and consistent security framework is of utmost importance to protect all EU personnel, data, communication networks, information systems and decision-making processes, thus also contributing to the democratic functioning of the European Union. A reinforced security culture of the Union institutions, bodies and agencies would also render Europe fit for the digital age and build a future-proof economy at the service of people.

AMENDMENTS

The Committee on Constitutional Affairs calls on the Committee on Industry, Research and Energy, as the committee responsible, to take into account the following amendments:

Amendment 1

Proposal for a regulation
Recital 1

Text proposed by the Commission	*Amendment*
(1) In the digital age, information and communication technology is a cornerstone in an open, efficient and independent Union administration. Evolving technology and increased complexity and interconnectedness of digital systems amplify cybersecurity risks making the Union administration more vulnerable to	(1) In the digital age, information and communication technology is a cornerstone in an open, efficient and independent Union administration. Evolving technology and increased complexity and interconnectedness of digital systems amplify cybersecurity risks making the Union administration more vulnerable to

cyber threats and incidents, which ultimately poses threats to the administration's business continuity and capacity to secure its data. While increased use of cloud services, ubiquitous use of ***IT***, high digitalisation, remote work and evolving technology and connectivity are nowadays core features of all activities of the Union administration entities, digital resilience is not yet sufficiently built in.	cyber threats and incidents, which ultimately poses threats to the administration's business continuity and capacity to secure its data. While increased use of cloud services, ***the*** ubiquitous use of ***information and communication technology ('ICT')***, high digitalisation, remote work and evolving technology and connectivity are nowadays core features of all activities of the Union administration entities, digital resilience is not yet sufficiently built in.

Justification

The Commission's proposal mentions "IT" where "ICT should instead be used as this is the standard term used in the NIS2 and the EU Cybersecurity Act.

Amendment 2

Proposal for a regulation
Recital 2

Text proposed by the Commission	*Amendment*
(2) The cyber threat landscape faced by Union institutions, bodies and agencies is in constant evolution. The tactics, techniques and procedures employed by threat actors are constantly evolving, while the prominent motives for such attacks change little, from stealing valuable undisclosed information to making money, manipulating public opinion or undermining digital infrastructure. The pace at which they conduct their cyberattacks keeps increasing, while their campaigns are increasingly sophisticated and automated, targeting exposed attack surfaces that keep expanding and quickly exploiting vulnerabilities.	(2) The cyber threat landscape faced by Union institutions, bodies***, offices*** and agencies is in constant evolution. The tactics, techniques and procedures employed by threat actors are constantly evolving, while the prominent motives for such attacks change little, from stealing valuable undisclosed information to making money, manipulating public opinion or undermining digital infrastructure. The pace at which they conduct their cyberattacks keeps increasing, while their campaigns ***and methods*** are increasingly sophisticated and automated, targeting exposed attack surfaces that keep expanding and quickly exploiting vulnerabilities.

Amendment 3

Proposal for a regulation

Recital 3

Text proposed by the Commission	*Amendment*
(3) The Union institutions, bodies and agencies' ***IT*** environments have interdependencies, integrated data flows and their users collaborate closely. This interconnection means that any disruption, even when initially confined to one Union institution, body or agency, can have cascading effects more broadly, potentially resulting in far-reaching and long-lasting negative impacts on the others. In addition, certain institutions, bodies and agencies' ***IT*** environments are connected with Member States' ***IT*** environments, causing an incident in one Union entity to pose a risk to the cybersecurity of Member States' ***IT*** environments and vice versa.	(3) The Union institutions, bodies***,*** ***offices*** and agencies' ***ICT*** environments have interdependencies, integrated data flows and their users collaborate closely. This interconnection means that any disruption, even when initially confined to one Union institution, body***, office*** or agency, can have cascading effects more broadly, potentially resulting in far-reaching and long-lasting negative impacts on the others. In addition, certain institutions, bodies***, offices*** and agencies' ***ICT*** environments are connected with Member States' ***ICT*** environments, causing an incident in one Union entity to pose a risk to the cybersecurity of Member States' ***ICT*** environments and vice versa.

Amendment 4
Proposal for a regulation
Recital 4

Text proposed by the Commission	*Amendment*
(4) The Union institutions, bodies and agencies are attractive targets who face highly skilled and well-resourced threat actors as well as other threats. At the same time, the level and maturity of cyber resilience and the ability to detect and respond to malicious cyber activities varies significantly across those entities. It is thus necessary for the functioning of the European administration that the institutions, bodies and agencies of the Union achieve a high common level of cybersecurity through a cybersecurity baseline (a set of minimum cybersecurity rules with which network and information systems and their operators and users have to be compliant to ***minimise*** cybersecurity risks), information exchange and collaboration.	(4) The Union institutions, bodies***,*** ***offices*** and agencies are attractive targets who face highly skilled and well-resourced threat actors as well as other threats. At the same time, the level and maturity of cyber resilience and the ability to detect and respond to malicious cyber activities varies significantly across those entities. It is thus necessary for the functioning of the European administration that the institutions, bodies***, offices*** and agencies of the Union achieve a high common level of cybersecurity through a cybersecurity baseline (a set of ***common,*** minimum cybersecurity rules with which network and information systems and their operators and users have to be compliant to ***limit*** cybersecurity risks), ***regular and effective*** information exchange and

collaboration***, and cybersecurity training***.

Amendment 5

Proposal for a regulation
Recital 7

Text proposed by the Commission	*Amendment*
(7) The differences between Union institutions, bodies and agencies require flexibility in the implementation since one size will not fit all. The measures for a high common level of cybersecurity should ***not include any obligations directly interfering with*** the exercise of the missions of Union institutions, bodies and agencies ***or encroaching on*** their institutional autonomy. Thus, those institutions, bodies and agencies should establish their own frameworks for cybersecurity risk management, governance and control, and adopt their own baselines and cybersecurity plans.	(7) The differences between Union institutions, bodies***, offices*** and agencies require flexibility in the implementation since one size will not fit all. The measures for a high common level of cybersecurity should ***support*** the exercise of the missions of Union institutions, bodies***, offices*** and agencies ***and take into account*** their institutional autonomy. Thus, those institutions, bodies***, offices*** and agencies should establish their own frameworks for cybersecurity risk management, governance and control, and adopt their own baselines and cybersecurity plans***, taking into account the coherence and interoperability of their respective frameworks and based on the common framework set by this Regulation***.

Amendment 6
Proposal for a regulation
Recital 8

Text proposed by the Commission	*Amendment*
(8) In order to avoid imposing a disproportionate financial and administrative burden on Union institutions, bodies and agencies, the cybersecurity risk management requirements should ***be proportionate*** to the risk presented by the network and information system concerned, taking into account the state of the art of such measures. Each Union institution, body and agency should aim to allocate ***an adequate percentage*** of its ***IT*** budget to improve its	(8) In order to avoid imposing a disproportionate financial and administrative burden on Union institutions, bodies***, offices*** and agencies, the cybersecurity risk management requirements should ***correspond*** to the risk presented by the network and information system concerned, taking into account the state of the art of such measures. Each Union institution, body***, office*** and agency should aim to allocate ***at least 10%*** of its ***ICT*** budget to improve its level of

level of cybersecurity***;*** in the ***longer term a target*** in the ***order of 10% should be pursued***.

cybersecurity in the ***medium term and more*** in the ***long term if necessary***.

Amendment 7

Proposal for a regulation
Recital 9

Text proposed by the Commission	*Amendment*
(9) A high common level of cybersecurity requires cybersecurity to come under the oversight of the highest level of management of each Union institution, body and agency, who should approve a cybersecurity baseline that should address the risks identified under the framework to be established by each institution, body and agency. Addressing the cybersecurity culture, i.e. the daily practice of cybersecurity, ***is*** an integral part of a cybersecurity baseline in all Union institutions, bodies and agencies.	(9) A high common level of cybersecurity requires cybersecurity to come under the oversight of ***an EU common board with*** the highest level of management of each Union institution, body***, office*** and agency, who should approve a cybersecurity baseline that should address the risks identified under the framework to be established by each institution, body***, office*** and agency. Addressing the cybersecurity culture, i.e. the daily practice of cybersecurity, ***should become*** an integral part of a cybersecurity baseline in all Union institutions, bodies***, offices*** and agencies.

Amendment 8

Proposal for a regulation
Recital 10

Text proposed by the Commission	*Amendment*
(10) Union institutions, bodies and agencies should assess risks related to relationships with suppliers and service providers, including providers of data storage and processing services or managed security services, and take appropriate measures to address them. These measures should form part of the cybersecurity baseline and be further specified in guidance documents or recommendations issued by CERT-EU. When defining measures and guidelines,	(10) Union institutions, bodies***, offices*** and agencies should assess risks related to relationships with suppliers and service providers, including providers of data storage and processing services or managed security services, and take appropriate measures to address them***. Those suppliers and service providers should be vetted thoroughly, taking into account the full range of the supply chain and economic and political environment in which they operate. Where the***

due account should be taken of relevant EU legislation and policies, including risk assessments and recommendations issued by the NIS Cooperation Group, such as the EU Coordinated risk assessment and EU Toolbox on 5G cybersecurity. In addition, certification of relevant ICT products, services and processes ***could*** be required, under specific EU cybersecurity certification schemes adopted pursuant to Article 49 of Regulation EU 2019/881.

relationships with such suppliers and service providers pose a risk to the integrity of democratic processes in the Union, they should be terminated without undue delay. These measures should form part of the cybersecurity baseline and be further specified in guidance documents or recommendations issued by CERT-EU. When defining measures and guidelines, due account should be taken of relevant EU legislation and policies, including risk assessments and recommendations issued by the NIS Cooperation Group, such as the EU Coordinated risk assessment and EU Toolbox on 5G cybersecurity. In addition, ***considering the threat landscape and the importance of building up resilience,*** certification of relevant ICT products, services and processes ***used in Union institutions, bodies, offices and agencies should*** be required, under specific EU cybersecurity certification schemes adopted pursuant to Article 49 of Regulation EU 2019/881.

Amendment 9

Proposal for a regulation
Recital 13

Text proposed by the Commission	*Amendment*
(13) Many cyberattacks are part of wider campaigns that target groups of Union institutions, bodies and agencies or communities of interest that include Union institutions, bodies and agencies. To enable proactive detection, incident response or mitigating measures, Union institutions, bodies and agencies should notify CERT-EU of significant cyber threats, significant vulnerabilities and significant incidents and share appropriate technical details that enable detection or mitigation of, as well as response to, similar cyber threats, vulnerabilities and incidents in other Union institutions, bodies and agencies.	(13) Many cyberattacks are part of wider campaigns that target groups of Union institutions, bodies***, offices*** and agencies or communities of interest that include Union institutions, bodies***, offices*** and agencies. To enable proactive detection, incident response or mitigating measures, Union institutions, bodies***, offices*** and agencies should notify CERT-EU of significant cyber threats, significant vulnerabilities and significant incidents and share appropriate technical details that enable detection or mitigation of, as well as response to, similar cyber threats, vulnerabilities and incidents in other Union

Following the same approach as the one envisaged in Directive [proposal NIS 2], where entities become aware of a significant incident they should be required to submit an ***initial notification*** to CERT-EU within 24 hours. Such information exchange should enable CERT-EU to disseminate the information to other Union institutions, bodies and agencies, as well as to appropriate counterparts, to help protect the Union ***IT*** environments and the Union's counterparts' ***IT*** environments against similar incidents, threats and vulnerabilities.	institutions, bodies***, offices*** and agencies. Following the same approach as the one envisaged in Directive [proposal NIS 2], where entities become aware of a significant incident they should be required to submit an ***early warning*** to CERT-EU ***without undue delay and in any event no later than*** 24 hours***. The Union institutions, bodies, offices and agencies should be allocated sufficient resources to fulfil their reporting obligations quickly and efficiently to ensure that the system designed works correctly***. Such information exchange should enable CERT-EU to disseminate the information to other Union institutions, bodies***, offices*** and agencies, as well as to appropriate counterparts, to help protect the Union ***ICT*** environments and the Union's counterparts' ***ICT*** environments against similar incidents, threats and vulnerabilities.

Amendment 10

Proposal for a regulation
Recital 14

Text proposed by the Commission	*Amendment*
(14) In addition to giving CERT-EU more tasks and an expanded role, an Interinstitutional Cybersecurity Board (IICB) should be established, which should facilitate a high common level of cybersecurity among Union institutions, bodies and agencies by monitoring the implementation of this Regulation by the Union institutions, bodies and agencies and by supervising implementation of general priorities and objectives by CERT-EU and providing strategic direction to CERT-EU. The IICB should ensure representation of the institutions and include representatives of agencies and bodies through the Union Agencies Network.	(14) In addition to giving CERT-EU more tasks and an expanded role, an Interinstitutional Cybersecurity Board (IICB) should be established, which should facilitate a high common level of cybersecurity among Union institutions, bodies***, offices*** and agencies by monitoring the implementation of this Regulation by the Union institutions, bodies***, offices*** and agencies and by supervising implementation of general priorities and objectives by CERT-EU and providing strategic direction to CERT-EU. The IICB should ensure ***an equal*** representation of the institutions and include representatives of agencies***, offices*** and bodies through the Union Agencies Network.

Amendment 11

Proposal for a regulation
Recital 16

Text proposed by the Commission	*Amendment*
(16) The IICB should monitor compliance with this Regulation as well as follow-up of guidance documents and recommendations, and calls for action issued by CERT-EU. The IICB should be supported on technical matters by technical advisory groups ***composed as the IICB sees fit*** which should work in close cooperation with CERT-EU, the Union institutions, bodies and agencies and other stakeholders as ***necessary***. Where necessary, the IICB should issue ***non-binding*** warnings and ***recommend*** audits.	(16) The IICB should monitor compliance with this Regulation as well as follow-up of guidance documents and recommendations, and calls for action issued by CERT-EU. The IICB should be supported on technical matters by technical advisory groups, which should work in close cooperation with CERT-EU, the Union institutions, bodies***, offices*** and agencies and other stakeholders as ***appropriate***. Where necessary, the IICB should issue warnings and ***recommendations for*** audits.

Amendment 12

Proposal for a regulation
Recital 17

Text proposed by the Commission	*Amendment*
(17) CERT-EU should have the mission to contribute to the security of the ***IT*** environment of all Union institutions, bodies and agencies. CERT-EU should act as the equivalent of the designated coordinator for the Union institutions, bodies and agencies, for the purpose of coordinated vulnerability disclosure to the European vulnerability registry as referred to in Article 6 of Directive [proposal NIS 2].	(17) CERT-EU should have the mission to contribute to the security of the ***ICT*** environment of all Union institutions, bodies***, offices*** and agencies. CERT-EU should act as the equivalent of the designated coordinator for the Union institutions, bodies***, offices*** and agencies, for the purpose of coordinated vulnerability disclosure to the European vulnerability registry as referred to in Article 6 of Directive [proposal NIS 2].

Amendment 13

Proposal for a regulation
Recital 18

Text proposed by the Commission	*Amendment*
(18) In 2020, CERT-EU's Steering Board set a new strategic aim for CERT-EU to guarantee a comprehensive level of cyber defence for all Union institutions, bodies and agencies with suitable breadth and depth and continuous adaptation to current or impending threats, including attacks against mobile devices, cloud environments and internet-of-things devices. The strategic aim also includes broad-spectrum Security Operations Centres (SOCs) that monitor networks, and 24/7 monitoring for high-severity threats. For the larger Union institutions, bodies and agencies, CERT-EU should support their ***IT*** security teams, including with first-line 24/7 monitoring. For smaller and some medium-sized Union institutions, bodies and agencies, CERT-EU should provide all the services.	(18) In 2020, CERT-EU's Steering Board set a new strategic aim for CERT-EU to guarantee a comprehensive level of cyber defence for all Union institutions, bodies***, offices*** and agencies with suitable breadth and depth and continuous adaptation to current or impending threats, including attacks against mobile devices, cloud environments and internet-of-things devices. The strategic aim also includes broad-spectrum Security Operations Centres (SOCs) that monitor networks, and 24/7 monitoring for high-severity threats. For the larger Union institutions, bodies***, offices*** and agencies, CERT-EU should support their ***ICT*** security teams, including with first-line 24/7 monitoring. For smaller and some medium-sized Union institutions, bodies***, offices*** and agencies, CERT-EU should provide all the services.

Amendment 14

Proposal for a regulation
Recital 19 a (new)

Text proposed by the Commission	*Amendment*
	(19a) In order to ensure a better implementation of cybersecurity measures and guidelines for Union institutions, bodies, offices and agencies, and to consolidate a culture of cybersecurity therein, CERT-EU should also enhance cooperation with the European Cybersecurity Competence Network and Centre.

Amendment 15

Proposal for a regulation
Recital 20

Text proposed by the Commission	*Amendment*
(20) In supporting operational cybersecurity, CERT-EU should make use of the available expertise of the European Union Agency for Cybersecurity through structured cooperation as provided for in Regulation (EU) 2019/881 of the European Parliament and of the Council[5] . ***Where appropriate,*** dedicated arrangements between the two entities should be established to define the practical implementation of such cooperation and to avoid the duplication of activities. CERT-EU should cooperate with the European Union Agency for Cybersecurity on threat analysis and share its threat landscape report with the Agency on a regular basis.	(20) In supporting operational cybersecurity, CERT-EU should make use of the available expertise of the European Union Agency for Cybersecurity through structured cooperation as provided for in Regulation (EU) 2019/881 of the European Parliament and of the Council. Dedicated arrangements between the two entities should be established to define the practical implementation of such cooperation and to avoid the duplication of activities. CERT-EU should cooperate with the European Union Agency for Cybersecurity on threat analysis and share its threat landscape report with the Agency on a regular basis.
[5] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15).	[5] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15).

Amendment 16
Proposal for a regulation
Recital 24

Text proposed by the Commission	*Amendment*
(24) As the services and tasks of CERT-EU are in the interest of all Union institutions, bodies and agencies, each Union institution, body and agency with ***IT*** expenditure should contribute ***a fair share*** to those services and tasks. Those contributions are without prejudice to the budgetary ***autonomy*** of the Union institutions, bodies and agencies.	(24) As the services and tasks of CERT-EU are in the interest of all Union institutions, bodies***, offices*** and agencies, each Union institution, body***, office*** and agency with ***ICT*** expenditure should contribute ***proportionally*** to those services and tasks. Those contributions are without prejudice to the budgetary ***capacity*** of the Union institutions, bodies***, offices*** and agencies.

Amendment 17

Proposal for a regulation
Recital 25

Text proposed by the Commission	*Amendment*
(25) The IICB, with the assistance of CERT-EU, should review and evaluate the implementation of this Regulation and should report its findings to the Commission. Building on this input, the Commission should report to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions.	(25) The IICB, with the assistance of CERT-EU, should review and evaluate the implementation of this Regulation and should report its findings to the Commission. Building on this input, the Commission should report***, at least every three years,*** to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions.

Amendment 18

Proposal for a regulation
Article 1 – paragraph 1 – point a

Text proposed by the Commission	*Amendment*
(a) obligations on Union institutions, bodies and agencies to establish an internal cybersecurity risk management, governance and control framework;	(a) obligations on Union institutions, bodies***, offices*** and agencies to establish an internal cybersecurity risk management, governance and control framework;

Amendment 19

Proposal for a regulation
Article 1 – paragraph 1 – point c

Text proposed by the Commission	*Amendment*
(c) rules on the organisation and operation of the Cybersecurity Centre for the Union institutions, bodies and agencies (CERT-EU) and on the organisation and operation of the Interinstitutional Cybersecurity Board.	(c) rules on the organisation and operation of the Cybersecurity Centre for the Union institutions, bodies***, offices*** and agencies (CERT-EU) and on the ***functioning,*** organisation and operation of the Interinstitutional Cybersecurity Board ***(IICB)***.

Amendment 20

Proposal for a regulation
Article 2 a (new)

Text proposed by the Commission	*Amendment*
	Article 2a
	Processing of personal data
	The processing of personal data under this Regulation by CERT-EU, the IICB and all Union institutions, bodies, offices and agencies shall be carried out in accordance with Regulation (EU) 2018/1725 of the European Parliament and of the Council.

Amendment 21

Proposal for a regulation
Article 3 – paragraph 1 – point 2

Text proposed by the Commission	*Amendment*
(2) 'network and information system' means network and information system ***within the meaning of Article 4(1)*** of Directive [proposal NIS 2];	(2) 'network and information system' means network and information system ***as defined in Article 6, point*** (1), of Directive [proposal NIS 2];

Amendment 22

Proposal for a regulation
Article 3 – paragraph 1 – point 4

Text proposed by the Commission	*Amendment*
(4) **'**cybersecurity' means cybersecurity ***within the meaning of*** Article ***4(3)*** of ***Directive [proposal NIS 2];***	(4) 'cybersecurity' means cybersecurity ***as defined in*** Article ***2, point (1),*** of ***Regulation (EU) 2019/881 of the European Parliament and of the Council***[1a]
	[1a] 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).

Amendment 23

Proposal for a regulation
Article 3 – paragraph 1 – point 5

Text proposed by the Commission	*Amendment*
(5) 'highest level of management' means a manager, management or coordination and oversight body at the most senior administrative level, taking account of the high-level governance arrangements in each Union institution, body or agency;	(5) 'highest level of management' means a manager, management or coordination and oversight body at the most senior administrative level ***with a mandate to make or authorise decisions***, taking account of the high-level governance arrangements in each Union institution, body***,*** ***office*** or agency;

Amendment 24

Proposal for a regulation
Article 3 – paragraph 1 – point 7

Text proposed by the Commission	*Amendment*
(7) 'significant incident' means any incident ***unless it*** has ***limited impact and is likely to be already well understood in terms of method or technology;***	(7) 'significant incident' means any incident which has caused or is capable of causing severe operational disruption to the functioning of the Union entity or financial loss for the Union entity concerned or which has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage;

Amendment 25

Proposal for a regulation
Article 3 – paragraph 1 – point 11

Text proposed by the Commission	*Amendment*
(11) 'significant cyber threat' means a	(11) 'significant cyber threat' means a

cyber threat ***with the intention, opportunity and capability to cause a significant incident***;	cyber threat ***as defined in Article 6, point (11), of Directive [proposal NIS 2]***;

Amendment 26

Proposal for a regulation
Article 3 – paragraph 1 – point 14

Text proposed by the Commission	*Amendment*
(14) '***cybersecurity*** risk' means any ***reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems***;	(14) 'risk' means any ***risk as defined in Article 6, point (9), of Directive [proposal NIS 2]***;

Amendment 27

Proposal for a regulation
Article 3 – paragraph 1 – point 14 a (new)

Text proposed by the Commission	*Amendment*
	(14a) 'ICT environment' means any on-premise or virtual ICT product, ICT service and ICT process as defined in Article 2, points (12), (13) and (14) of Regulation (EU) 2019/881, and any network and information system whether owned and operated by a Union institution, body, office or agency, or hosted or operated by a third party, including mobile devices, corporate networks, and business networks not connected to the internet and any devices connected to the ICT environment;

Justification

Term moved from Article 4(2) of this Proposal to Article on Definitions given that this term is consistently used throughout the text. The suggested definition for this term draws from the definitions of its components from Article 2 of the Cyber Security Act Regulation (EU) 2019/881.

Amendment 28

Proposal for a regulation
Article 3 – paragraph 1 – point 15

Text proposed by the Commission	*Amendment*
(15) 'Joint Cyber Unit' means a virtual and physical platform for cooperation for the different cybersecurity communities in the Union, with a focus on operational and technical coordination against major cross-border cyber threats and incidents within the meaning of Commission Recommendation of 23 June 2021;	***deleted***

Amendment 29
Proposal for a regulation
Article 4 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Each Union institution, body and agency shall establish its own internal cybersecurity risk management, governance and control framework ('the framework') in support of the entity's mission and exercising its institutional autonomy. This work shall be overseen by the entity's highest level of management ***to ensure*** an effective and prudent management of all cybersecurity risks. The framework shall be in place by …. at the latest [15 months after the entry into force of this Regulation].	1. ***Based on a full security audit,*** each Union institution, body***, office*** and agency shall establish its own internal cybersecurity risk management, governance and control framework ('the framework') in support of the entity's mission and exercising its institutional autonomy***, whilst also taking into account the coherence and interoperability of their framework with those of other relevant institutions, bodies, offices and agencies***. This work shall be overseen by the entity's highest level of management***, which shall be responsible for ensuring*** an effective and prudent management of all cybersecurity risks. The framework shall be in place by …. at the latest [15 months after the ***date of*** entry into force of this Regulation].

Amendment 30

Proposal for a regulation
Article 4 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The framework shall cover the entirety of the ***IT*** environment of the concerned institution, body or agency, including any on-premise ***IT*** environment, outsourced assets and services in cloud computing environments or hosted by third parties, mobile devices, corporate networks, business networks not connected to the internet and any devices connected to the ***IT*** environment. The framework shall take account of business continuity and crisis management and it shall consider supply chain security as well as the management of human risks that could impact the cybersecurity of the concerned Union institution, body or agency.	2. The framework shall cover the entirety of the ***ICT*** environment of the concerned institution, body***, office*** or agency, including any on-premise ***ICT*** environment, outsourced assets and services in cloud computing environments or hosted by third parties, mobile devices, corporate networks, business networks not connected to the internet and any devices connected to the ***ICT*** environment. The framework shall take account of business continuity and crisis management and it shall consider supply chain security as well as the management of human risks that could impact the cybersecurity of the concerned Union institution, body***, office*** or agency.

Amendment 31
Proposal for a regulation
Article 4 – paragraph 4

Text proposed by the Commission	*Amendment*
4. Each Union institution, body and agency shall have effective mechanisms in place to ensure that ***an adequate percentage*** of the ***IT*** budget is spent on cybersecurity.	4. Each Union institution, body***, office*** and agency shall have effective mechanisms in place to ensure that ***at least 10 %*** of the ***aggregated ICT*** budget is spent on cybersecurity ***in the medium term***.

Amendment 32

Proposal for a regulation
Article 4 – paragraph 5 a (new)

Text proposed by the Commission	*Amendment*
	5a. The Local Cybersecurity Officer shall cooperate with the data protection officer referred to in Article 43 of Regulation (EU) 2018/1725, when dealing with overlapping activities applying data protection by design and by default to cybersecurity measures, and when

selecting cybersecurity measures that involve protection of personal data, integrated risk management and integrated security incident handling.

Amendment 33

Proposal for a regulation
Article 5 – paragraph 1

Text proposed by the Commission	*Amendment*
1. The highest level of management of each Union institution, body and agency shall approve the entity's own cybersecurity baseline to address the risks identified under the framework referred to in Article 4(1). It shall do so in support of its mission and exercising its institutional autonomy. The cybersecurity baseline shall be in place by …. at the latest [18 months after the entry into force of this Regulation] and shall address the domains listed in Annex I and the measures listed in Annex II.	1. The highest level of management of each Union institution, body***, office*** and agency shall approve the entity's own cybersecurity baseline to address the risks identified under the framework referred to in Article 4(1). It shall do so in support of its mission and exercising its institutional autonomy ***in full compliance with the requirements of this Regulation, and taking into account the coherence and interoperability of its framework with those of other relevant institutions, bodies, offices and agencies as well as the guidance documents and recommendations adopted by the IICB on a proposal from CERT-EU and the applicable EU cybersecurity certification schemes***. The cybersecurity baseline shall be in place by …. at the latest [18 months after the ***date of*** entry into force of this Regulation] and shall address the domains listed in Annex I and the measures listed in Annex II.

Amendment 34

Proposal for a regulation
Article 5 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The senior management of each Union institution, body and agency shall follow specific trainings on a regular basis	2. The senior management of each Union institution, body***, office*** and agency shall follow specific trainings on a regular

to gain sufficient knowledge and skills in order to apprehend and assess cybersecurity risk and management practices and their impact on the operations of the organisation.	basis to gain sufficient knowledge and skills in order to apprehend and assess cybersecurity risk and management practices and their impact on the operations of the organisation ***with proper resources***. ***In addition to such specific trainings and for the purpose of building and consolidating cybersecurity culture, regular cybersecurity training of staff members shall be included in the cybersecurity plan and updated at least every two years. Sufficient resources shall be ensured to provide quality training.***

Amendment 35

Proposal for a regulation
Article 6 – paragraph 1

Text proposed by the Commission	*Amendment*
Each Union institution, body and agency shall carry out a cybersecurity maturity assessment at least every ***three*** years, incorporating all the elements of their ***IT*** environment as described in Article 4, taking account of the relevant guidance documents and recommendations adopted in accordance with Article 13.	Each Union institution, body***, office*** and agency shall carry out a cybersecurity maturity assessment ***by ... [6 months after the entry into force of this Regulation], and*** at least every ***two*** years ***thereafter***, incorporating all the elements of their ***ICT*** environment as described in Article 4, taking account of the relevant guidance documents and recommendations adopted in accordance with Article 13. ***The maturity assessment shall be based on independent cybersecurity audits by vetted providers.***

Amendment 36

Proposal for a regulation
Article 7 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Following the conclusions derived from the maturity assessment and considering the assets and risks identified pursuant to Article 4, the highest level of	1. Following the conclusions derived from the maturity assessment and considering the assets and risks identified pursuant to Article 4, the highest level of

management of each Union institution, body and agency shall approve a cybersecurity plan without undue delay after the establishment of the risk management, governance and control framework and the cybersecurity baseline. The plan shall aim at increasing the overall cybersecurity of the concerned entity and shall thereby contribute to the achievement or enhancement of a high common level of cybersecurity among all Union institutions, bodies and agencies. To support the entity's mission on the basis of its institutional autonomy, the plan shall at least include the domains listed in Annex I, the measures listed in Annex II, as well as measures related to incident preparedness, response and recovery, such as security monitoring and logging. The plan shall be revised at least every ***three*** years, following the maturity assessments carried out pursuant to Article 6.	management of each Union institution, body***, office*** and agency shall approve a cybersecurity plan without undue delay after the establishment of the risk management, governance and control framework and the cybersecurity baseline. The plan shall aim at increasing the overall cybersecurity of the concerned entity and shall thereby contribute to the achievement or enhancement of a high common level of cybersecurity among all Union institutions, bodies***, offices*** and agencies. To support the entity's mission on the basis of its institutional autonomy, the plan shall at least include the domains listed in Annex I, the measures listed in Annex II, as well as measures related to incident preparedness, response and recovery, such as security ***assessment of the suppliers and services,*** monitoring and logging. The plan shall be revised at least every ***two*** years, following the maturity assessments carried out pursuant to Article 6.

Amendment 37

Proposal for a regulation
Article 7 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The cybersecurity plan shall include staff members' roles and responsibilities for its implementation.	2. The cybersecurity plan shall include staff members' roles***, preparedness*** and responsibilities for its implementation.

Amendment 38

Proposal for a regulation
Article 7 – paragraph 3

Text proposed by the Commission	*Amendment*
3. The cybersecurity plan shall ***consider any*** applicable guidance documents and recommendations issued by CERT-EU.	3. The cybersecurity plan shall ***include all proposed measures contained in the*** applicable guidance documents and recommendations issued by CERT-EU.

Amendment 39

Proposal for a regulation
Article 7 – paragraph 3 a (new)

Text proposed by the Commission	*Amendment*
	3 a. The Union institutions, bodies, offices and agencies shall submit their cybersecurity plans to the IICB. These plans shall be shared to the extent possible without risking the reveal or disclosure of sensitive or confidential information about the particular technical cybersecurity arrangements and capabilities of the Union entity to unauthorised third parties.

Amendment 40

Proposal for a regulation
Article 9 – paragraph 2 – point a

Text proposed by the Commission	*Amendment*
(a) monitoring the implementation of this Regulation by the Union institutions, bodies and agencies;	(a) monitoring the implementation of this Regulation by the Union institutions, bodies***, offices*** and agencies ***and making recommendations for achieving a common high level of cybersercurity***;

Amendment 41

Proposal for a regulation
Article 9 – paragraph 3 – subparagraph 1 – introductory part

Text proposed by the Commission	*Amendment*
The IICB shall consist of three representatives nominated by the Union Agencies Network (EUAN) upon a proposal of its ICT Advisory Committee to represent the interests of the agencies and bodies that run their own ***IT*** environment and one representative designated by each	The IICB shall consist of three representatives nominated by the Union Agencies Network (EUAN) upon a proposal of its ICT Advisory Committee to represent the interests of the ***offices,*** agencies and bodies that run their own ***ICT*** environment and one representative

of the following:	designated by each of the following:

Amendment 42

Proposal for a regulation
Article 9 – paragraph 3 – subparagraph 1 – point k a (new)

Text proposed by the Commission	*Amendment*
	(ka) the European Data Protection Supervisor.

Amendment 43

Proposal for a regulation
Article 10 – paragraph 1 – point a a (new)

Text proposed by the Commission	*Amendment*
	(aa) approve, on the basis of a proposal from the Head of CERT-EU, recommendations for achieving a common high level of cybersecurity, aimed at one or all Union institutions, bodies, offices and agencies;

Amendment 44

Proposal for a regulation
Article 11 – paragraph 1 – point a

Text proposed by the Commission	*Amendment*
(a) issue a warning; where necessary in view of a compelling cybersecurity risk, the audience of the warning shall be restricted appropriately;	(a) issue a warning; where necessary in view of a compelling cybersecurity risk, the audience of the warning shall be restricted appropriately***, through a commonly agreed methodology***;

Amendment 45

Proposal for a regulation
Article 11 – paragraph 1 – point b

Text proposed by the Commission	*Amendment*
(b) ***recommend*** a relevant audit service to carry out an audit.	(b) ***instruct*** a relevant audit service to carry out an audit.

Amendment 46

Proposal for a regulation
Article 12 – paragraph 1

Text proposed by the Commission	*Amendment*
1. The mission of CERT-EU, the autonomous interinstitutional Cybersecurity Centre for all Union institutions, bodies and agencies, shall be to contribute to the security of the unclassified ***IT*** environment of all Union institutions, bodies and agencies by advising them on cybersecurity, by helping them to prevent, detect, mitigate and respond to incidents and by acting as their cybersecurity information exchange and incident response coordination hub.	1. The mission of CERT-EU, the autonomous interinstitutional Cybersecurity Centre for all Union institutions, bodies***, offices*** and agencies, shall be to contribute to the security of the unclassified ***ICT*** environment of all Union institutions, bodies***, offices*** and agencies by advising them on cybersecurity, by helping them to prevent, detect, mitigate and respond to incidents and by acting as their cybersecurity information exchange and incident response coordination hub.

Amendment 47

Proposal for a regulation
Article 12 – paragraph 2 – point d

Text proposed by the Commission	*Amendment*
(d) raise to the attention of the IICB any issue relating to the implementation of this Regulation and of the implementation of the guidance documents, recommendations and calls for action;	(d) raise to the attention of the IICB any issue relating to the implementation of this Regulation and of the implementation of the guidance documents, recommendations and calls for action ***and make proposals for redress***;

Amendment 48

Proposal for a regulation
Article 12 – paragraph 4

Text proposed by the Commission	*Amendment*
4. CERT-EU shall engage in structured cooperation with the European Union Agency for Cybersecurity on capacity building, operational cooperation and long-term strategic analyses of cyber threats in accordance with Regulation (EU) 2019/881 of the European Parliament and of the Council.	4. CERT-EU shall engage in structured cooperation with the European Union Agency for Cybersecurity on capacity building, operational cooperation and long-term strategic analyses of cyber threats in accordance with Regulation (EU) 2019/881 of the European Parliament and of the Council. ***Furthermore, CERT-EU may cooperate and exchange information with the European Cybercrime Centre.***

Amendment 49

Proposal for a regulation
Article 12 – paragraph 5 – introductory part

Text proposed by the Commission	*Amendment*
5. CERT-EU may provide the following services not described in its service catalogue (‘chargeable services’):	5. CERT-EU may provide ***Union institutions, bodies, offices and agencies with*** the following services not described in its service catalogue (‘chargeable services’):

Amendment 50

Proposal for a regulation
Article 12 – paragraph 5 – point a

Text proposed by the Commission	*Amendment*
(a) services that support the cybersecurity of Union institutions, bodies and agencies’ ***IT*** environment, other than those referred to in paragraph 2, on the basis of service level agreements and subject to available resources;	(a) services that support the cybersecurity of Union institutions, bodies***,*** ***offices*** and agencies’ ***ICT*** environment, other than those referred to in paragraph 2, on the basis of service level agreements and subject to available resources;

Amendment 51

Proposal for a regulation
Article 12 – paragraph 5 – point b

Text proposed by the Commission	*Amendment*
(b) services that support cybersecurity operations or projects of Union institutions, bodies and agencies, other than those to protect their ***IT*** environment, on the basis of written agreements and with the prior approval of the IICB;	(b) services that support cybersecurity operations or projects of Union institutions, bodies***, offices*** and agencies, other than those to protect their ***ICT*** environment, on the basis of written agreements and with the prior approval of the IICB;

Amendment 52
Proposal for a regulation
Article 12 – paragraph 5 – point c

Text proposed by the Commission	*Amendment*
(c) services that support the security of their ***IT*** environment to organisations other than the Union institutions, bodies and agencies that cooperate closely with Union institutions, bodies and agencies, for instance by having assigned tasks or responsibilities under Union law, on the basis of written agreements and with the prior approval of the IICB.	(c) services that support the security of their ***ICT*** environment to organisations other than the Union institutions, bodies***, offices*** and agencies that cooperate closely with Union institutions, bodies***, offices*** and agencies, for instance by having assigned tasks or responsibilities under Union law, on the basis of written agreements and with the prior approval of the IICB.

Amendment 53

Proposal for a regulation
Article 12 – paragraph 6

Text proposed by the Commission	*Amendment*
6. CERT-EU may organise cybersecurity exercises or recommend participation in existing exercises, in close cooperation with the European Union Agency for Cybersecurity whenever applicable, to test the level of cybersecurity of the Union institutions, bodies and agencies.	6. CERT-EU may organise cybersecurity exercises or recommend participation in existing exercises, in close cooperation with the European Union Agency for Cybersecurity whenever applicable, to test the level of cybersecurity of the Union institutions, bodies***, offices*** and agencies ***on a regular basis***. ***Moreover, through enhanced cooperation***

	and joint programmes with the European Cyber Cybersecurity Competence Network and Centre (ECCC), CERT-EU may support research and innovation and aid in strengthening the cybersecurity capabilities of the Union institutions, bodies, offices and agencies.

Amendment 54

Proposal for a regulation
Article 12 – paragraph 7

Text proposed by the Commission	*Amendment*
7. CERT-EU ***may*** provide assistance to Union institutions, bodies and agencies regarding incidents in classified ***IT*** environments if it is explicitly requested to do so by the ***constituent*** concerned.	7. CERT-EU ***shall*** provide assistance to Union institutions, bodies***, offices*** and agencies regarding incidents in classified ***ICT*** environments if it is explicitly requested to do so by the ***Union institutions, bodies, offices or agencies*** concerned ***and if CERT -EU has the required resources to do so or receives such resources from the entity concerned***.

Amendment 55

Proposal for a regulation
Article 14 – paragraph 1

Text proposed by the Commission	*Amendment*
The Head of CERT-EU shall ***regularly*** submit reports to the IICB and the IICB Chair on the performance of CERT-EU, financial planning, revenue, implementation of the budget, service level agreements and written agreements entered into, cooperation with counterparts and partners, and missions undertaken by staff, including the reports referred to in Article 10(1).	The Head of CERT-EU shall***, at least once a year,*** submit reports to the IICB and the IICB Chair on the performance of CERT-EU, financial planning, revenue, implementation of the budget, service level agreements and written agreements entered into, cooperation with counterparts and partners, and missions undertaken by staff, including the reports referred to in Article 10(1).

Amendment 56

Proposal for a regulation
Article 16 – paragraph 1

Text proposed by the Commission	*Amendment*
1. CERT-EU shall cooperate and exchange information with national counterparts in the Member States, including CERTs, National Cybersecurity Centres, CSIRTs, and single points of contact referred to in Article 8 of Directive [proposal NIS 2], on cyber threats, vulnerabilities and incidents, on possible countermeasures and on all matters relevant for improving the protection of the ***IT*** environments of Union institutions, bodies and agencies, including through the CSIRTs network referred to in Article 13 of Directive [proposal NIS 2].	1. CERT-EU shall cooperate and exchange information with national counterparts in the Member States, including CERTs, National Cybersecurity Centres, CSIRTs, and single points of contact referred to in Article 8 of Directive [proposal NIS 2], on cyber threats, vulnerabilities and incidents, on possible countermeasures and on all matters relevant for improving the protection of the ***ICT*** environments of Union institutions, bodies***, offices*** and agencies, including through the CSIRTs network referred to in Article 13 of Directive [proposal NIS 2].

Amendment 57

Proposal for a regulation
Article 16 – paragraph 2

Text proposed by the Commission	*Amendment*
2. CERT-EU may exchange incident-specific information with national counterparts in the Member States to facilitate detection of similar cyber threats or incidents without the consent of the affected ***constituent***. CERT-EU may only exchange incident-specific information which reveals the identity of the target of the cybersecurity incident with the consent of the affected ***constituent***.	2. CERT-EU may exchange incident-specific information with national counterparts in the Member States to facilitate detection of similar cyber threats or incidents without the consent of the affected ***Union institutions, bodies, offices or agencies, as long as the processing of personal data complies with the applicable provisions of Regulation (EU) 2018/1725***. CERT-EU may only exchange incident-specific information, which reveals the identity of the target of the cybersecurity incident with the consent of the affected ***Union institutions, bodies, offices or agencies***.

Amendment 58

Proposal for a regulation
Article 17 – paragraph 1

Text proposed by the Commission	*Amendment*
1. CERT-EU may cooperate with non-Member State counterparts including industry sector-specific counterparts on tools and methods, such as techniques, tactics, procedures and best practices, and on cyber threats and vulnerabilities. For all cooperation with such counterparts, including in frameworks where non-EU counterparts cooperate with national counterparts of Member States, CERT-EU shall seek prior approval from the IICB.	1. CERT-EU may cooperate with non-Member State counterparts including industry sector-specific counterparts***,*** on tools and methods, such as techniques, tactics, procedures and best practices, and on cyber threats and vulnerabilities. For all cooperation with such counterparts, including in frameworks where non-EU counterparts cooperate with national counterparts of Member States, CERT-EU shall seek prior approval from the IICB. ***Any such cooperation shall respect the democratic integrity of the EU.***

Amendment 59

Proposal for a regulation
Article 17 – paragraph 2

Text proposed by the Commission	*Amendment*
2. CERT-EU may cooperate with other partners, such as commercial entities, international organisations, non-European Union national entities or individual experts, to gather information on general and specific cyber threats, vulnerabilities and possible countermeasures. For wider cooperation with such partners, CERT-EU shall seek prior approval from the IICB.	2. CERT-EU may cooperate with other partners, such as commercial entities, international organisations, non-European Union national entities or individual experts, to gather information on general and specific cyber threats, vulnerabilities and possible countermeasures. For wider cooperation with such partners, CERT-EU shall seek prior approval from the IICB. ***Any such cooperation shall respect the democratic integrity of the EU.***

Amendment 60

Proposal for a regulation
Article 17 – paragraph 3

Text proposed by the Commission	*Amendment*
3. CERT-EU may, with the consent of the ***constituent*** affected by an incident, provide information related to the incident to partners that can contribute to its	3. CERT-EU may, with the consent of the ***Union institutions, bodies, offices or agencies*** affected by an incident, provide information related to the incident to

analysis.	partners that can contribute to its analysis.

Amendment 61

Proposal for a regulation
Article 19 – paragraph -1 (new)

Text proposed by the Commission	*Amendment*
	-1. Union institutions, bodies, offices or agencies may voluntarily provide CERT-EU with information on cyber threats, incidents, near misses and vulnerabilities affecting them. CERT-EU shall ensure that efficient means of communication are available for the purpose of facilitating information sharing with the Union entities. CERT-EU may prioritise the processing of mandatory notifications over voluntary notifications.

Amendment 62

Proposal for a regulation
Article 19 – paragraph 1

Text proposed by the Commission	*Amendment*
1. To ***enable CERT-EU to coordinate vulnerability management and incident response, it*** may request Union institutions, bodies and agencies to provide it with information from their respective ***IT*** system inventories ***that is relevant for the CERT-EU support***. The requested ***institution, body or agency*** shall transmit the requested information, and any subsequent updates thereto, without undue delay.	1. To ***perform its mission and tasks as defined in Article 12, CERT-EU*** may request Union institutions, bodies, offices and agencies to provide it with information from their respective ***ICT*** system inventories***, including information relating to cyber threats, near misses, vulnerabilities, indicators of compromise, cybersecurity alerts and recommendations regarding the configuration of cybersecurity tools to detect cyber incidents***. The requested ***entity*** shall transmit the requested information, and any subsequent updates thereto, without undue delay.

Amendment 63

Proposal for a regulation
Article 19 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The Union ***institutions, bodies and agencies***, upon request from CERT-EU and without undue delay, shall provide it with digital information created by the use of electronic devices involved in their respective incidents. CERT-EU may further clarify which types of such digital information it requires for situational awareness and incident response.	2. The Union institutions, bodies***, offices*** and agencies, upon request from CERT-EU and without undue delay, shall provide it with digital information created by the use of electronic devices involved in their respective incidents. CERT-EU may further clarify which types of such digital information it requires for situational awareness and incident response.

Amendment 64
Proposal for a regulation
Article 20 – title

Text proposed by the Commission	*Amendment*
Notification obligations	***Reporting*** obligations

Amendment 65

Proposal for a regulation
Article 20 – paragraph 1 – subparagraph 1

Text proposed by the Commission	*Amendment*
All Union institutions, bodies and agencies shall ***make an initial notification*** to CERT-EU of significant cyber threats, significant vulnerabilities and significant incidents without undue delay and in any event no later than 24 hours after becoming aware of them.	All Union institutions, bodies***, offices*** and agencies shall ***provide an early warning*** to CERT-EU of significant cyber threats, significant vulnerabilities and significant incidents without undue delay and in any event no later than 24 hours after becoming aware of them. ***That early warning shall, where applicable, indicate whether the significant incident is presumably caused by unlawful or malicious action and whether it has or could have a cross-border impact***.

Amendment 66

Proposal for a regulation
Article 20 – paragraph 1 – subparagraph 2

Text proposed by the Commission	*Amendment*
In duly justified cases and in agreement with CERT-EU, the Union institution, body or agency concerned ***can*** deviate from ***the*** deadline ***laid down in the previous paragraph***.	In duly justified cases and in agreement with CERT-EU, the Union institution, body***, office*** or agency concerned ***may*** deviate from ***that*** deadline.

Amendment 67

Proposal for a regulation
Article 20 – paragraph 2 – introductory part

Text proposed by the Commission	*Amendment*
2. The Union institutions, bodies and agencies shall further ***notify*** to CERT-EU without undue delay appropriate technical details of cyber threats, vulnerabilities and incidents that enable detection, incident response or mitigating measures. The notification shall include if available:	2. The Union institutions, bodies***, offices*** and agencies shall further ***send a notification*** to CERT-EU without undue delay***, and in any event within 72 hours after having become aware of the significant incident, update the early warning and provide an initial assessment of the significant incident, its severity and impact, with the*** appropriate technical details of cyber threats, vulnerabilities and incidents that enable detection, incident response or mitigating measures. The notification shall include if available:

Amendment 68
Proposal for a regulation
Article 20 – paragraph 2 – subparagraph 1 a (new)

Text proposed by the Commission	*Amendment*
	In duly justified cases and in agreement with CERT-EU, the Union institution, body, office or agency concerned may deviate from this deadline.

Amendment 69

Proposal for a regulation
Article 20 – paragraph 2 a (new)

Text proposed by the Commission	*Amendment*
	2 a. No later than one month after submitting the notification on a significant incident, the Union institutions, bodies, offices and agencies shall submit a final report to CERT-EU, including at least the following:
	(a) a detailed description of the significant incident, its severity and impact;
	(b) the type of threat or root cause that likely triggered the significant incident;;
	(c) applied and ongoing mitigation measures;
	(d) where applicable, the cross-border impact of the significant incident.
	Where the significant incident is still ongoing at the time of the submission of the final report referred to in the first subparagraph, a progress report at that time and a final report within one month after the incident shall be submitted.

Amendment 70

Proposal for a regulation
Article 20 – paragraph 2 b (new)

Text proposed by the Commission	*Amendment*
	2 b. In duly justified cases, and in agreement with CERT-EU, the Union institution, body, office or agency concerned may deviate from the deadline laid down in paragraph 2a.

Amendment 71

Proposal for a regulation
Article 20 – paragraph 3

Text proposed by the Commission	*Amendment*
3. CERT-EU shall submit to ENISA on a monthly basis a summary report including anonymised and aggregated data on significant cyber threats, significant vulnerabilities and significant incidents notified in accordance with paragraph 1.	3. CERT-EU shall submit to ENISA on a monthly basis a summary report including anonymised and aggregated data on significant cyber threats, significant vulnerabilities and significant incidents notified in accordance with paragraph 1. ***That report shall constitute an input to the biennial report on the state of cybersecurity in the Union under Article 18 of Directive [proposal NIS 2].***

Amendment 72

Proposal for a regulation
Article 20 – paragraph 4

Text proposed by the Commission	*Amendment*
4. The IICB ***may*** issue guidance documents or recommendations concerning the modalities and content of the notification. CERT-EU shall disseminate the appropriate technical details to enable proactive detection, incident response or mitigating measures by Union institutions, bodies and agencies.	4. The IICB ***shall*** issue guidance documents or recommendations concerning the modalities and content of the notification. CERT-EU shall disseminate the appropriate technical details to enable proactive detection, incident response or mitigating measures by Union institutions, bodies***, offices*** and agencies.

Amendment 73

Proposal for a regulation
Article 20 – paragraph 5

Text proposed by the Commission	*Amendment*
5. The notification obligations shall not extend to EUCI and to information that a Union institution, body or agency has received from a Member State Security or Intelligence Service or law enforcement agency under the explicit condition that it will not be shared with	***deleted***

CERT-EU.

Amendment 74

Proposal for a regulation
Article 24 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The Commission shall report on the implementation of this Regulation to the European Parliament and the Council at the latest ***48*** months after the entry into force of this Regulation and every ***three*** years thereafter.	2. The Commission shall report on the implementation of this Regulation to the European Parliament and the Council at the latest ***36*** months after the entry into force of this Regulation and every ***two*** years thereafter.

Amendment 75

Proposal for a regulation
Article 24 – paragraph 3

Text proposed by the Commission	*Amendment*
3. The Commission shall evaluate the functioning of this Regulation and report to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions no sooner than ***five*** years after the date of entry into force.	3. The Commission shall evaluate the functioning of this Regulation and report to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions no sooner than ***three*** years after the date of entry into force***, given the rapidly evolving cyber threat landscape***.

Amendment 76

Proposal for a regulation
Annex I – paragraph 1 – introductory part

Text proposed by the Commission	*Amendment*
The following domains shall be addressed in the cybersecurity baseline:	***At least*** the following domains shall be addressed in the cybersecurity baseline:

Amendment 77

Proposal for a regulation
Annex I – paragraph 1 – point 1 a (new)

Text proposed by the Commission	*Amendment*
	(1 a) cybersecurity training of staff members;

Amendment 78

Proposal for a regulation
Annex I – paragraph 1 – point 3

Text proposed by the Commission	*Amendment*
(3) asset management, including ***IT*** asset inventory and ***IT*** network cartography;	(3) asset ***acquisition and*** management, including ***ICT*** asset inventory and ***ICT*** network cartography;

Amendment 79

Proposal for a regulation
Annex I – paragraph 1 – point 7

Text proposed by the Commission	*Amendment*
(7) system acquisition, development and maintenance;	(7) system acquisition, development and maintenance***, including in-house open source software development***;

Amendment 80

Proposal for a regulation
Annex I – paragraph 1 – point 7 a (new)

Text proposed by the Commission	*Amendment*
	(7a) cybersecurity audits;

Amendment 81

Proposal for a regulation
Annex I – paragraph 1 – point 9

Text proposed by the Commission	*Amendment*
(9) incident management, including approaches to improve the preparedness, response to and recovery from incidents and cooperation with CERT-EU, such as the maintenance of security monitoring and logging;	(9) incident management, including approaches to improve the preparedness, response to and recovery from incidents, ***compliance with and shortening timescales for reporting obligations*** and cooperation with CERT-EU, such as the maintenance of security monitoring and logging;

Amendment 82

Proposal for a regulation
Annex II – paragraph 1 – point 3 a (new)

Text proposed by the Commission	*Amendment*
	(3 a) regular cybersecurity training of staff members;

Amendment 83

Proposal for a regulation
Annex II – paragraph 1 – point 4 – point a

Text proposed by the Commission	*Amendment*
(a) the removal of contractual barriers that limit information sharing from ***IT*** service providers about incidents, vulnerabilities and cyber threats with CERT-EU;	(a) the removal of contractual barriers that limit information sharing from ***ICT*** service providers about incidents, vulnerabilities and cyber threats with CERT-EU;

PROCEDURE – COMMITTEE ASKED FOR OPINION

Title	Laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union
References	COM(2022)0122 – C9-0122/2022 – 2022/0085(COD)
Committee responsible Date announced in plenary	ITRE 4.4.2022
Opinion by Date announced in plenary	AFCO 4.4.2022
Rapporteur for the opinion Date appointed	Markéta Gregorová 20.6.2022
Discussed in committee	26.10.2022 1.12.2022
Date adopted	25.1.2023
Result of final vote	+: 24 –: 0 0: 0
Members present for the final vote	Gerolf Annemans, Gabriele Bischoff, Damian Boeselager, Gwendoline Delbos-Corfield, Salvatore De Meo, Daniel Freund, Charles Goerens, Esteban González Pons, Laura Huhtasaari, Victor Negrescu, Max Orville, Domènec Ruiz Devesa, Helmut Scholz, Pedro Silva Pereira, Sven Simon, Guy Verhofstadt, Loránt Vincze, Rainer Wieland
Substitutes present for the final vote	Nathalie Colin-Oesterlé, Pascal Durand, Seán Kelly, Jaak Madison, Maite Pagazaurtundúa
Substitutes under Rule 209(7) present for the final vote	Leszek Miller

FINAL VOTE BY ROLL CALL IN COMMITTEE ASKED FOR OPINION

24	+
ID	Gerolf Annemans, Laura Huhtasaari, Jaak Madison
PPE	Nathalie Colin-Oesterlé, Salvatore De Meo, Esteban González Pons, Seán Kelly, Sven Simon, Loránt Vincze, Rainer Wieland
Renew	Charles Goerens, Max Orville, Maite Pagazaurtundúa, Guy Verhofstadt
S&D	Gabriele Bischoff, Pascal Durand, Leszek Miller, Victor Negrescu, Domènec Ruiz Devesa, Pedro Silva Pereira
The Left	Helmut Scholz
Verts/ALE	Damian Boeselager, Gwendoline Delbos-Corfield, Daniel Freund

0	-

0	0

Key to symbols:
+ : in favour
- : against
0 : abstention