European Parliament
2019-2024

Plenary sitting

A9-0064/2023

10.3.2023

***I
REPORT

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))

Committee on Industry, Research and Energy

Rapporteur: Henna Virkkunen

Rapporteur for the opinion of the associated committee pursuant to Rule 57 of the Rules of Procedure
Tomas Tobé, Committee on Civil Liberties, Justice and Home Affairs

Symbols for procedures

*	Consultation procedure
***	Consent procedure
***I	Ordinary legislative procedure (first reading)
***II	Ordinary legislative procedure (second reading)
***III	Ordinary legislative procedure (third reading)

(The type of procedure depends on the legal basis proposed by the draft act.)

Amendments to a draft act

Amendments by Parliament set out in two columns

Deletions are indicated in ***bold italics*** in the left-hand column. Replacements are indicated in ***bold italics*** in both columns. New text is indicated in ***bold italics*** in the right-hand column.

The first and second lines of the header of each amendment identify the relevant part of the draft act under consideration. If an amendment pertains to an existing act that the draft act is seeking to amend, the amendment heading includes a third line identifying the existing act and a fourth line identifying the provision in that act that Parliament wishes to amend.

Amendments by Parliament in the form of a consolidated text

New text is highlighted in ***bold italics***. Deletions are indicated using either the ▌ symbol or strikeout. Replacements are indicated by highlighting the new text in ***bold italics*** and by deleting or striking out the text that has been replaced.
By way of exception, purely technical changes made by the drafting departments in preparing the final text are not highlighted.

CONTENTS

Page

DRAFT EUROPEAN PARLIAMENT LEGISLATIVE RESOLUTION

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))

(Ordinary legislative procedure: first reading)

The European Parliament,

– having regard to the Commission proposal to Parliament and the Council (COM(2022)0122),

– having regard to Article 294(2) and Articles 298 of the Treaty on the Functioning of the European Union, pursuant to which the Commission submitted the proposal to Parliament (C9-0122/2022),

– having regard to Article 294(3) of the Treaty on the Functioning of the European Union,

– having regard to Rule 59 of its Rules of Procedure,

– having regard to the opinions of the Committee on Civil Liberties, Justice and Home Affairs, the Committee on Budgets and the Committee on Constitutional Affairs,

– having regard to the report of the Committee on Industry, Research and Energy (A9-0064/2023),

1. Adopts its position at first reading hereinafter set out;

2. Calls on the Commission to refer the matter to Parliament again if it replaces, substantially amends or intends to substantially amend its proposal;

3. Instructs its President to forward its position to the Council, the Commission and the national parliaments.

Amendment 1

AMENDMENTS BY THE EUROPEAN PARLIAMENT*

to the Commission proposal

2022/0085 (COD)

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

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 298 thereof,

Having regard to the Treaty establishing the European Atomic Energy Community, and in particular Article 106a thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Acting in accordance with the ordinary legislative procedure,

Whereas:

(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

* Amendments: new or amended text is highlighted in bold italics; deletions are indicated by the symbol ▌.

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.

(2) The cyber threat landscape faced by Union ***entities*** 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.

(3) The Union ***entities' 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 ***entity***, can have cascading effects more broadly, potentially resulting in far-reaching and long-lasting negative impacts on the others. In addition, certain ***Union entities' 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.

(4) The Union ***entities*** 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 ***Union entities*** achieve a high common level of cybersecurity through ***the implementation of*** cybersecurity ***risk-management measures commensurate with the relevant*** risks ▌, information exchange and collaboration.

(5) ▌ Directive ***(EU) 2022/2555 of the European Parliament and of the Council***[1] aims to further improve the cybersecurity resilience and incident response capacities of public

[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).***

and private entities, national competent authorities and bodies as well as the Union as a whole. It is therefore necessary that Union ***entities*** follow suit by ensuring rules that are consistent with ▌ Directive ***(EU) 2022/2555*** and mirror its level of ambition.

(6) To reach a high common level of cybersecurity, it is necessary that each Union ***entity*** establishes ***a*** cybersecurity risk management, ***handling of incidents,*** governance and control framework that ensures an effective and prudent management of all cybersecurity risks, and takes account of business continuity and crisis management. ***That framework should lay down cybersecurity policies and priorities for the security of network and information systems encompassing the entirety of the ICT environment. The framework should be reviewed on a regular basis and at least every three years.***

(7) The differences between Union ***entities*** 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 ***entities*** or encroaching on their institutional autonomy. ***Therefore***, those ***entities*** should establish their own frameworks for cybersecurity risk management, ***handling of incidents,*** governance and control, and adopt their own ***cybersecurity risk-management measures*** and cybersecurity plans***, covering the entity's entire ICT environment***. ***Union entities should continuously evaluate the effectiveness of the adopted risk-management measures and their proportionality relative to the identified risks, and where necessary, adjust and revise accordingly their frameworks and plans on the basis of the results of the cybersecurity maturity assessments.***

(7a) The recurrent obligation to carry out cybersecurity maturity assessments could create an additional and disproportionate burden for small Union entities with limited ICT resources. This Regulation should therefore provide for the possibility for two or more Union entities to create joint teams for carrying out the cybersecurity maturity assessments, and benefit from combining resources and expertise.

(8) In order to avoid imposing a disproportionate financial and administrative burden on Union ***entities***, 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 ***entity*** should aim

to allocate an adequate percentage of its ***ICT*** budget to improve its level of cybersecurity; in the longer term a target in the order of ***at least*** 10 % should be pursued.

(9) A high common level of cybersecurity requires cybersecurity to come under the oversight of the highest level of management of each Union ***entity***, who should ***oversee the implementation of the provisions of this Regulation and*** approve ***the establishment, and any subsequent revisions thereof, of the risk management and control framework, the corresponding*** cybersecurity ***risk-management measures addressing*** the risks identified ***in*** the framework ***and the cybersecurity plans of*** each ***Union entity***. Addressing the cybersecurity culture, i.e. the daily practice of cybersecurity, is an integral part of a cybersecurity ***risk management, governance and control framework and the corresponding cybersecurity risk-management measures*** in all Union ***entities***.

(10) Union ***entities*** 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 ▌ cybersecurity ***risk-management measures should*** be further specified in guidance documents or recommendations issued by CERT-EU. When defining measures and guidelines, due account should be taken of relevant ***Union law*** and policies, including risk assessments and recommendations issued by the ▌ Cooperation Group ***established by Directive (EU) 2022/2555***, 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 for the Union entities*** certification of relevant ICT products, services and processes ***must*** be required, under specific ***Union*** cybersecurity certification schemes adopted pursuant to Article 49 of Regulation EU 2019/881.

(11) In May 2011, the Secretaries-General of the Union institutions and bodies decided to establish a pre-configuration team for a computer emergency response team for the Union's institutions, bodies and agencies (CERT-EU) supervised by an inter-institutional Steering Board. In July 2012, the Secretaries-General confirmed the practical arrangements and agreed to maintain CERT-EU as a permanent entity to continue to help improve the overall level of information technology security of the Union's institutions, bodies and agencies as an example of visible inter-institutional cooperation in cybersecurity. In September 2012, CERT-EU was established as a

Taskforce of the European Commission with an interinstitutional mandate. In December 2017, the Union institutions and bodies concluded an interinstitutional arrangement on the organisation and operation of CERT-EU[2]. ***That*** arrangement should continue to evolve to support the implementation of this Regulation ***and should be evaluated on a regular basis in light of future negotiations of long-term budget frameworks allowing for further decisions to be made with respect to the functioning and institutional role of CERT-EU, including the possible establishment of CERT-EU as a Union office***.

(12) CERT-EU should be renamed from 'computer emergency response team' to 'Cybersecurity Centre' for the Union ***entities***, in line with developments in the Member States and globally, where many CERTs are renamed as Cybersecurity Centres, but it should keep the short name 'CERT-EU' because of name recognition.

(13) Many cyberattacks are part of wider campaigns that target groups of Union ***entities*** or communities of interest that include Union ***entities***. To enable proactive detection, incident response or mitigating measures, ***and recovery from significant incidents, Union entities*** should notify CERT-EU of significant cyber threats, significant vulnerabilities***, near misses*** and significant incidents and share appropriate technical details that enable detection or mitigation of, as well as response to ***and recovery from*** similar ▌ incidents in other Union ***entities***. Following the same approach as the one envisaged in Directive ***(EU) 2022/2555***, where entities become aware of a significant incident they should be required to submit an ***early warning*** to CERT-EU within 24 hours. Such information exchange should enable CERT-EU to disseminate the information to other Union ***entities***, 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.

(13a) This Regulation lays down a multiple-stage approach to the reporting of significant incidents in order to strike the right balance between, on the one hand, swift reporting that helps to mitigate the potential spread of incidents and that allows Union entities to seek assistance, and, on the other, in-depth reporting that draws valuable lessons from individual incidents and improves over time the resilience of individual Union entities and contributes to increasing the overall cybersecurity posture of Union administration. In that regard, this Regulation should include the reporting of

[2] OJ C 12, 13.1.2018, p. 1 ▌.

incidents that, based on an initial assessment performed by the Union entity concerned, could cause severe operational disruption of the services or financial loss for that Union entity or affect other natural or legal persons by causing considerable material or non-material damage. Such initial assessment should take into account, inter alia, the network and information systems affected, in particular their importance for the functioning and operations of the Union entity concerned, the severity and technical characteristics of a cyber threat and any underlying vulnerabilities that are being exploited as well as the experience of the Union entity concerned with similar incidents. Indicators such as the extent to which the functioning of Union entity is affected, the duration of an incident or the number of users affected could play an important role in identifying whether the operational disruption of the service is severe.

(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 ***entities*** by monitoring the implementation of this Regulation by the Union ***entities*** 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.

(14a) The IICB aims to support entities in elevating their respective cybersecurity postures by implementing this Regulation. In order to support Union entities, the IICB should adopt guidance and recommendations required for Union entities' cybersecurity maturity assessments and cybersecurity plans, review possible interconnections between Union entities' ICT environments and support the establishment of a Cybersecurity Officers Group under ENISA, comprising the Local Cybersecurity Officers of all Union entities with an aim to facilitate the sharing of best practices and experiences gained from the implementation of this Regulation.

(14b) In order to ensure consistency with Directive (EU) 2022/2555, the IICB could adopt recommendations on the basis of the results of Union level coordinated security risk assessments of critical supply chains referred to in Article 22 of Directive (EU) 2022/2555 to support Union entities in adopting effective and proportionate risk-management measures relating to supply chain security and develop guidelines for

information sharing arrangements of Union entities relating to the voluntary notification of cyber threats, near misses and incidents to CERT-EU.

(15) CERT-EU should support the implementation of measures for a high common level of cybersecurity through proposals for guidance documents and recommendations to the IICB or by issuing calls for action. Such guidance documents and recommendations should be approved by the IICB. When needed, CERT-EU should issue calls for action describing urgent security measures which Union ***entities*** are urged to take within a set timeframe.

(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 ***entities*** and other stakeholders as ***appropriate***. Where necessary, the IICB should issue ▌ warnings and ***requests for*** audits.

(16a) Where the IICB finds that a Union entity has not effectively applied or implemented this Regulation, it could, without prejudice to the internal procedures of the Union entity concerned, request relevant and available documentation relating to the effective implementation of the provisions of this Regulation, communicate a reasoned opinion with observed gaps in the implementation of this Regulation, invite the Union entity concerned to provide a self-assessment on its reasoned opinion and issue, in cooperation with CERT-EU, guidance to bring its respective risk management, governance and control framework, cybersecurity risk-management measures, cybersecurity plans and reporting obligations in compliance with this Regulation.

(17) CERT-EU should have the mission to contribute to the security of the ***ICT*** environment of all Union ***entities***. ***Where appropriate, and in coordination with the Union entities, CERT-EU may submit to the IICB for its approval, a proposal for a coordinated cyber insurance policy covering Union entities, in order to establish first and third-party coverage to address the potential impact of incidents.*** CERT-EU should act as the ▌designated coordinator for the Union ***entities***, for the purpose of coordinated vulnerability disclosure to the European vulnerability ***database*** as referred to in Article ***12*** of Directive ***(EU) 2022/2555***.

(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 ***entities*** 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 ***entities***, CERT-EU should support their ***ICT*** security teams, including with first-line 24/7 monitoring. For smaller and some medium-sized Union ***entities***, CERT-EU should provide all the services.

(19) CERT-EU should also fulfil the role provided for it in Directive ***(EU) 2022/2555*** concerning cooperation and information exchange with the computer security incident response teams (CSIRTs) network. Moreover, in line with Commission Recommendation (EU) 2017/1584[3], CERT-EU should cooperate and coordinate on the response with the relevant stakeholders. In order to contribute to a high level of cybersecurity across the Union, CERT-EU should share incident specific information with national counterparts. CERT-EU should also collaborate with other public as well as private counterparts, including at NATO, subject to prior approval by the IICB.

(20) In supporting operational cybersecurity, CERT-EU should make use of the available expertise of the European Union Agency for Cybersecurity ***(ENISA)*** through structured cooperation as provided for in Regulation (EU) 2019/881 of the European Parliament and of the Council[4]. ▌Dedicated arrangements between the two entities should be established ***within two years of the date of entry into force of this Regulation,*** to define the practical implementation of such cooperation and to avoid the duplication of activities. CERT-EU should cooperate with ***ENISA*** on threat analysis and share its threat landscape report with the Agency on a regular basis.

---

3 Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises (OJ L 239, 19.9.2017, p. 36).

4 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).

(21) In support of the Joint Cyber Unit built in accordance with the Commission Recommendation of 23 June 2021[5], CERT-EU should cooperate and exchange information with stakeholders to foster operational cooperation and to enable the existing networks in realising their full potential in protecting the Union.

(22) All personal data processed under this Regulation should be processed in accordance with data protection ***law*** including Regulation (EU) 2018/1725 of the European Parliament and of the Council ▌[6]***. This Regulation should not affect the application of Union law governing the processing of personal data, including the tasks conferred on and powers of the European Data Protection Supervisor (EDPS). CERT-EU and the IICB should work in close cooperation with the EPDS and the staff specialised in data protection in the Union entities to ensure full compliance with Union data protection law.***

(22a) Cybersecurity systems and services involved in the prevention, detection and response to cyber threats should comply with data protection and privacy law and should take relevant technical and organisational safeguarding measures to ensure that such compliance is achieved in an accountable way.

(22b) Open-source cybersecurity tools and applications can contribute to a higher degree of openness. Open standards facilitate interoperability between security tools, benefitting the security of stakeholders. Open-source cybersecurity tools and applications can leverage the wider developer community, enabling diversification of suppliers. Open source can lead to a more transparent verification process of cybersecurity related tools and a community-driven process of discovering vulnerabilities. Union entities should therefore be able to promote the use of open-source software and open standards by pursuing policies relating to the use of open data and open-source as part of security through transparency.

---

5 Commission Recommendation C(2021) 4520 of 23.6.2021 on building a Joint Cyber Unit.

6 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

(23) The handling of information by CERT-EU and the Union ***entities*** should be in line with the rules ***on information security, in particular those*** laid down in Regulation [proposed Regulation on information security]. To ensure coordination on security matters, any contacts with CERT-EU initiated or sought by national security and intelligence services should be communicated to the Commission's Security Directorate and the chair of the IICB without undue delay.

(24) As the services and tasks of CERT-EU are in the interest of all Union ***entities***, each Union ***entity*** with ***ICT*** expenditure should contribute a fair share to those services and tasks. Those contributions are without prejudice to the budgetary autonomy of the Union ***entities***.

(24a) This Regulation should take into account the fact that, apart from the Union institutions, most of Union entities, in particular the small ones, do not have the necessary financial and human resources to be dedicated for additional cybersecurity tasks.

(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.

HAVE ADOPTED THIS REGULATION:

Chapter I

GENERAL PROVISIONS

Article 1

Subject-matter

This Regulation lays down measures that aim to achieve a high common level of cybersecurity in Union entities. To that end, this Regulation lays down:

(a) obligations ***that require Union entities*** to establish ***a*** cybersecurity risk management, ***handling of incidents,*** governance and control framework;

(b) cybersecurity risk management and reporting obligations for Union ***entities***;

(ba) rules underpinning information sharing obligations and the facilitation of voluntary information sharing arrangements with regard to Union entities;

(c) rules on the organisation***, tasks*** and operation of the Cybersecurity Centre for the Union ***entities*** (CERT-EU) and on the ***functioning,*** organisation and operation of the Interinstitutional Cybersecurity Board ***(IICB)***.

Article 2

Scope

This Regulation applies to ▌ all Union ***entities*** and to the ***functioning,*** organisation and operation of CERT-EU and the ***IICB***.

Article 3

Definitions

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

(1) 'Union ***entities'*** means the Union institutions, bodies***, offices*** and agencies set up by, or on the basis of, the Treaty on European Union, the Treaty on the functioning of European Union or the Treaty establishing the European Atomic Energy Community;

(2) 'network and information system' means network and information system ***as defined in Article 6, point (1),*** of Directive ***(EU) 2022/2555***;

(3) 'security of network and information systems' means security of network and information systems ***as defined in Article 6, point (2),*** of Directive ***(EU) 2022/2555***;

(4) 'cybersecurity' means cybersecurity ***as defined in Article 2, point (1), of Regulation (EU) 2019/881***;

(5) 'highest level of management' means a manager, management or coordination and oversight body ***responsible for the functioning of the Union entity concerned,*** at the most senior administrative level, ***with a mandate to adopt or authorise decisions in line with*** the high-level governance arrangements ***of the entity concerned, without***

prejudice to the formal responsibilities of other levels of management for compliance and risk management in their respective areas of responsibility;

(5a) 'near miss' means a near miss as defined in Article 6, point (5), of Directive (EU) 2022/2555;

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

▌

(8) 'major ***incident***' means ***an*** incident ***whose disruption exceeds an*** affected Union ***entity's and CERT-EU's capacity to respond to it, or which has a significant impact on at least two Union entities, or where a large-scale cybersecurity incident as defined in Article 6, point (7), of Directive (EU) 2022/2555 has a significant impact on at least one Union entity***;

(9) 'incident handling' means incident handling ***as defined in Article 6, point (8),*** of Directive ***(EU) 2022/2555***;

(10) 'cyber threat' means cyber threat ***as defined in Article 2, point (8),*** of Regulation (EU) 2019/881;

(11) 'significant cyber threat' means a cyber threat ***as defined in Article 6, point (11), of Directive (EU) 2022/2555***;

(12) 'vulnerability' means vulnerability ***as defined in*** Article ***6, point (15),*** of Directive ***(EU) 2022/2555***;

(13) 'significant vulnerability' means a vulnerability that will likely lead to a significant incident if it is exploited;

(14) '▌ risk' means ***a risk as defined in Article 6, point (9), of Directive (EU) 2022/2555***;

(14a) 'standard' means a standard as defined in Article 2, point (1), of Regulation (EU) No 1025/2012 of the European Parliament and of the Council[8];

---

[8] Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and

(14b) 'technical specification' means a technical specification as defined in Article 2, point (4), of Regulation (EU) No 1025/2012;

(14c) 'ICT product' means an ICT product as defined in of Article 2, point (12), of Regulation (EU) 2019/881;

(14d) 'ICT service' means an ICT service as defined in Article 2, point (13), of Regulation (EU) 2019/881;

(14e) 'ICT process' means an ICT process as defined in Article 2, point (14), of Regulation (EU) 2019/881;

(14f) 'ICT environment' means any on-premise or virtual ICT product, ICT service and ICT process, any network and information system, whether owned and operated by a entity, 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 and any dislocated premises and decentralised offices, such as liaison offices, representative offices or local offices;

(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;

(16) 'cybersecurity ***measures***' means a set of minimum cybersecurity rules ***and measures*** with which network and information systems and their operators and users must be compliant, to minimise cybersecurity risks.

Chapter II

MEASURES FOR A HIGH COMMON LEVEL OF CYBERSECURITY

Article 4

Risk management, ***handling of incidents,*** governance and control ***framework***

Decision No 1673/2006/EC of the European Parliament and of the Council (OJ L 316, 14.11.2012, p. 12).

1. ***On the basis of a full cybersecurity audit,*** each Union ***entity*** shall establish its own ▌ cybersecurity risk management, ***handling of incidents,*** governance and control framework ('the framework') in support of the ***Union*** entity's mission and exercising its institutional autonomy. ***The establishment of the framework*** shall be overseen by the ***Union*** entity's highest level of management ***and shall be under its responsibility in order*** to ensure an effective and prudent management of all cybersecurity risks. The framework shall be ***established*** by … ▌ [15 months after the ***date of*** entry into force of this Regulation].

2. The framework shall cover the entirety of the ***ICT*** environment of the ***Union entity*** concerned ▌. 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 ***and all other relevant technical, operational and organisational risks*** that could ***have an*** impact ***on*** the cybersecurity of the ▌ Union ***entity concerned***.

2a. The framework referred to in paragraph 1 shall define strategic objectives to ensure a high level of cybersecurity in the Union entities. That framework shall lay down cybersecurity policies for the security of network and information systems encompassing the entirety of the ICT environment, and define the roles and responsibilities of staff of the Union entities tasked with ensuring the effective implementation of this Regulation. The framework shall also include the key performance indicators (KPIs) for measuring the effectiveness of the implementation based on the KPIs list referred to in Article 12(2), point (eb).

2b. The framework referred to in paragraph 1 shall be reviewed on a regular basis and at least every three years. The first such review shall be carried out by ... [three years after the date of entry into force of this Regulation]. Where appropriate and upon request of the IICB, a Union entity's framework shall be updated following guidance from CERT-EU on incidents identified or possible gaps observed in the implementation of this Regulation.

3. The highest level of management of each Union ***entity*** shall ***be responsible for the implementation and shall oversee*** the compliance ***and functioning*** of ***its*** organisation with the obligations related to ***the framework***, without prejudice to the formal responsibilities of other levels of management for compliance and risk management in their respective areas of responsibility***, such as data protection***.

4. Each Union ***entity*** shall have effective mechanisms in place to ensure that an adequate percentage of the ***ICT*** budget is spent on cybersecurity.

5. Each Union ***entity*** shall appoint a Local Cybersecurity Officer or an equivalent function who shall act as its single point of contact regarding all aspects of cybersecurity. ***Local Cybersecurity Officers may be shared by several Union entities.***

Article 5

Cybersecurity ***risk-management measures***

1. The highest level of management of each Union ***entity*** shall approve the ***Union*** entity's own cybersecurity ***risk-management measures*** to address the risks identified under the framework referred to in Article 4(1)***, in line with any guidance and recommendations of IICB and CERT-EU***. ***Taking into account the state-of-the-art and, where applicable, relevant European and international standards, or available European*** cybersecurity ***certificates as defined in Article 2, point (11), of Regulation (EU) 2019/881, those risk-management measures shall ensure a level of security of network and information systems across the entirety of the ICT environment commensurate to the risks identified under the framework referred to in Article 4(1). When assessing the proportionality of those*** measures***, due account shall be taken of the degree of the Union entity's exposure to risks, its size, the likelihood of occurrence of incidents and their severity, including their societal, economic and interinstitutional impact***.

1a. Union entities shall include at least the following domains in the implementation of the cybersecurity risk-management measures:

(a) cybersecurity policy, including measures needed to reach objectives and priorities referred to in Article 4 and paragraph 2a of this Article;

(b) policy objectives regarding the use of cloud computing services as defined in Article 6, point (30), of Directive (EU) 2022/2555 and technical arrangements to enable and sustain teleworking;

(c) in order to assess whether Union entities have sufficient control over the security of their ICT systems, a complete cybersecurity initial review, including a risk, vulnerability and threat assessment, and a penetration-test of the ICT

systems and devices of the Union entities to be carried out by a leading and verified third party external to the Union entities, such as a leading cybersecurity company, on ... [the date of entry into force of this Regulation] and every following year thereafter, which takes due account of the information security requirements of the relevant institutions;

(d) in light of the reviews referred to in point (c), mitigation of the reported risks and vulnerabilities in cybersecurity updates, and implementation of the recommendations by means of cybersecurity policy which may include the replacement of infected ICT systems;

(e) organisation of cybersecurity, including definition of roles and responsibilities;

(f) management of ICT environment, including ICT asset inventory and ICT network cartography;

(g) access control, identity management and privileged access management;

(h) operations security and human resources security;

(i) communications security;

(j) system acquisition, development, maintenance and transparency of the source code;

(k) cybersecurity audits;

(l) ICT staff workload and overall satisfaction;

(m) supply chain security and supplier relationships between Union entities and their direct suppliers and service providers;

(n) incident handling, including approaches to improve the preparedness, detection, analysis, and containment of, response to and recovery from incidents and cooperation with CERT-EU, such as the maintenance of security monitoring and logging;

(o) business continuity management and crisis management; and

(p) skills, education, awareness-raising, training programmes and exercises.

2. The senior management of each Union ***entity, as well as all relevant staff tasked with implementing the cybersecurity risk-management measures and obligations laid down in this Regulation,*** shall follow specific trainings on a regular 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 ***Union entity***.

2a. Union entities shall address at least the following specific measures and sub-controls in the implementation of the cybersecurity risk-management measures in their cybersecurity plans, in line with the guidance documents and recommendations of the IICB:

(a) concrete steps for moving towards Zero Trust Architecture within the meaning of a security model comprised of a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries;

(b) the adoption of multifactor authentication as a norm across network and information systems;

(c) the use of cryptography and encryption, and in particular end-to-end encryption, encryption in transit, and encryption at rest as well as secure digital signing;

(d) secured voice, video and text communications, and secured emergency communications systems, where appropriate;

(e) the establishment of frequent and ad-hoc scanning capabilities of endpoint devices and other components of the ICT environment to detect and remove malware software such as spyware;

(f) ensuring privacy by design and the enhanced security of all personal data;

(g) the establishment of software supply chain security through criteria for secure software development and evaluation;

(h) regular cybersecurity training of staff members;

(i) participation in interconnectivity risk analyses between the Union entities;

(j) the enhancement of procurement rules to facilitate a high common level of cybersecurity through:

(i) the removal of contractual barriers that limit information sharing from ICT service providers about incidents, vulnerabilities and cyber threats with CERT-EU;

(ii) the contractual obligation to report incidents, vulnerabilities, near misses and cyber threats as well as to have appropriate incidents response and monitoring in place;

(k) the establishment and adoption of training programmes on cybersecurity commensurate to the prescribed tasks and expected capabilities for the highest level of management and technical and operational staff.

2b. The IICB may recommend technical and methodological requirements of the domains and cybersecurity risk-management measures referred to in paragraphs 1a and 2a of this Article and, where necessary, recommend adaptations to reflect developments in cyberattack methods, cyber threats and technological progress, for the purpose of the review referred to in Article 24.

Article 6

Cybersecurity maturity assessments

1. Each Union ***entity*** shall carry out a cybersecurity maturity assessment ***by ... [18 months after the date of 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.

2. Small Union entities with similar tasks or structure may carry out a combined cybersecurity maturity assessment.

3. The IICB, after consulting the European Union Agency for Cybersecurity (ENISA) and upon receiving guidance from CERT-EU, shall by ... [one year after the date of entry into force of this Regulation], issue guidelines to Union entities for the purpose of carrying out cybersecurity maturity assessments. The cybersecurity maturity assessment shall be based on cybersecurity audits.

4. Upon request of the IICB, and with the explicit consent of the Union entity concerned, the results of a cybersecurity maturity assessment may be discussed within the IICB or within the established network of Local Cybersecurity Officers with a view to learning from experiences in the implementation of this Regulation and sharing best practices and results of use cases.

Article 7

Cybersecurity plans

1. Following the conclusions derived from the ***cybersecurity*** maturity assessment and considering the ▌ risks identified pursuant to Article 4, the highest level of management of each Union ***entity*** shall approve a cybersecurity plan without undue delay after the establishment of the ▌ framework and the cybersecurity ***risk-management measures***. ***The cybersecurity*** plan shall aim at increasing the overall cybersecurity of the ***Union*** entity ***concerned*** and shall thereby contribute to the achievement or enhancement of a high common level of cybersecurity ***within the*** Union ▌. To support the ***Union*** entity's mission on the basis of its institutional autonomy, the ***cybersecurity*** plan shall at least include the ***cybersecurity risk-management*** measures ***referred to in Article 5(1a) and (2a)***. The ***cybersecurity*** plan shall be revised at least every ***two*** years, ***or where necessary, with any substantial revision of the framework referred to in Article 4,*** following the ***cybersecurity*** maturity assessments carried out pursuant to Article 6.

2. The cybersecurity plan shall include ***relevant*** staff members' roles***, required level of competence*** and responsibilities for its implementation***, including detailed job descriptions for technical and operational staff as well as all relevant processes underpinning performance evaluation***.

2a. The cybersecurity plan shall include the Union entity's cyber crisis management plan for major incidents.

3. The cybersecurity plan shall consider any applicable guidance documents and recommendations issued by CERT-EU ***in accordance with Article 13 or any applicable or targeted recommendations issued by the IICB and CERT-EU***.

3a. The Union entities shall submit their cybersecurity plans to the IICB.

Article 8

Implementation

1. Upon completion of ***their respective cybersecurity*** maturity assessments ***referred to in Article 6 and the cybersecurity plans referred to in Article 7***, the Union ***entities*** shall submit ***them*** to the ***IICB***. ▌ Upon request of the ***IICB***, they shall report on specific aspects of this Chapter.

2. Guidance documents and recommendations, issued in accordance with Article 13, shall support the implementation of the provisions laid down in this Chapter.

Chapter III

IICB

Article 9

IICB

1. ▌ IICB ▌ is established.

2. The IICB shall be responsible for:

   (a) monitoring the implementation of this Regulation by the Union ***entities and providing recommendations for achieving a high common level of cybersecurity***;

   (b) supervising the implementation of general priorities and objectives by CERT-EU and providing strategic direction to CERT-EU.

3. The IICB shall consist of***:***

   (a) ***two*** representatives ▌ designated by each of the following:

      (i) the European Parliament;

      (ii) the Council of the European Union;

      (iii) the European Commission;

   (b) ***one representative designated by each of the following:***

      (i) the Court of Justice of the European Union;

(ii) the European Central Bank;

(iii) the European Court of Auditors;

(iv) the European External Action Service;

(v) the European Economic and Social Committee;

(vi) the European Committee of the Regions;

(vii) the European Investment Bank;

(viii) ENISA;

(ix) the European Data Protection Supervisor (EDPS);

(x) the European Cybersecurity Industrial, Technology and Research Competence Centre;

(xi) the European Union Agency for the Space Programme;

(c) one representative designated by the Union Agencies Network (EUAN) upon a proposal of its ICT Advisory Committee to represent the interests of the agencies, offices and bodies other than those referred to in points (b)(viii), (x) and (xi) and that runs its own ICT environment.

Gender balance shall be aimed at among the appointed representatives.

3a. Members may be assisted by an alternate. Other representatives of the organisations listed above or of other Union ***entities*** may be invited by the chair to attend IICB meetings without voting power.

3b. The head of CERT-EU and the chairs of the Cooperation Group, the CSIRTs network and the EU-CyCLONe, referred to in Articles 14, 15 and 16 of Directive (EU) 2022/2555, or their alternates, may participate in IICB meetings as observers. In exceptional cases, and in accordance with the internal rules of procedure of the IICB, the IICB may decide otherwise.

4. The IICB shall adopt its internal rules of procedure.

5. The IICB shall designate a chair, in accordance with its internal rules of procedure, from among its members for a period of four years. His or her alternate shall become a full member ***with voting rights*** of the IICB for the same duration.

6. The IICB shall meet at the initiative of its chair, ***and at least two times a year,*** at the request of CERT-EU or at the request of any of its members.

7. Each member of the IICB shall have one vote. The IICB's decisions shall be taken by simple majority except where otherwise provided for in this Regulation. The chair shall not vote except in the event of a tied vote where he or she may cast a deciding vote.

8. The IICB may act by a simplified written procedure initiated in accordance with the internal rules of procedure of the IICB. Under that procedure, the relevant decision shall be deemed approved within the timeframe set by the chair, except where a member objects.

▌

10. The secretariat of the IICB shall be provided by the Commission.

11. The ***representative*** nominated by the EUAN ▌ shall relay the IICB's decisions to the Union agencies and joint undertakings. Any Union agency and body shall be entitled to raise with the representatives or the chair of the IICB any matter which it considers should be brought to the IICB's attention.

▌

13. The IICB may nominate an Executive Committee to assist it in its work, and delegate some of its tasks and powers to it. The IICB shall lay down the rules of procedure of the Executive Committee, including its tasks and powers, and the terms of office of its members.

Article 10

Tasks of the IICB

When exercising its responsibilities, the IICB shall in particular:

(-a) support Union entities in implementing this Regulation with the aim to raise their respective levels of cybersecurity;

(-aa) effectively monitor the implementation of the obligations of this Regulation in Union entities without prejudice to their institutional autonomy and the overall institutional balance;

(-ab) provide strategic direction to the head of CERT-EU;

(a) ***request*** reports ▌ from CERT-EU on the state of implementation of this Regulation by the Union ***entities***;

(aa) approve, on the basis of a proposal from the head of CERT-EU, recommendations for achieving a high common level of cybersecurity, addressed to one or more Union entities;

(ab) establish a framework for conducting of peer reviews for the Union entities with a view of learning from shared experiences, strengthening mutual trust, achieving a high common level of cybersecurity, as well as enhancing Union entities' capabilities, to be conducted by cybersecurity technical experts designated by an entity different from the entity being reviewed;

(b) approve, on the basis of a proposal from the Head of CERT-EU, the annual work programme for CERT-EU and monitor its implementation;

(c) approve, on the basis of a proposal from the Head of CERT-EU, CERT-EU's service catalogue;

(d) approve, on the basis of a proposal submitted by the Head of CERT-EU, the annual financial planning of revenue and expenditure, including staffing, for CERT-EU activities;

(e) approve, on the basis of a proposal from the Head of CERT-EU, the modalities for service level agreements;

(f) examine and approve the annual report drawn up by the Head of CERT-EU covering the activities of, and management of funds by CERT-EU;

(g) approve and monitor ***KPIs*** for CERT-EU defined on a proposal by the Head of CERT-EU;

(h) approve cooperation arrangements, service level arrangements or contracts between CERT-EU and other entities pursuant to Article 17;

(ha) adopt guidance documents or recommendations on the basis of CERT-EU proposal;

(hb) where necessary, instruct CERT-EU to issue, withdraw or modify a proposal for guidance documents or recommendations, or a call for action;

(i) establish ▌ technical advisory groups ***with concrete tasks*** to assist the IICB's work, approve their terms of reference and designate their respective chairs***;***

(ia) review and upon request, following relevant guidance from CERT-EU, provide feedback to Union entities' regarding the cybersecurity maturity assessments referred to in Article 6 and cybersecurity plans referred to in Article 7;

(ib) facilitate the exchange of best practices among the Local Cybersecurity Officers; provide, where appropriate, the recommendations on their role within the Union entities;

(ic) review possible interconnections between Union entities' ICT environments and maintain an inventory of shared components of ICT products, ICT services and ICT processes;

(id) where appropriate, adopt recommendations on the interoperability of Union entities' ICT environments or components thereof;

(ie) support the establishment of a Cybersecurity Officers Group, to be coordinated by ENISA, comprising the Local Cybersecurity Officers of all Union entities with an aim to facilitate the sharing of best practices and experiences gained from the implementation of this Regulation;

(if) develop an incident and response plan for major incidents and coordinate the adoption of individual Union entities' cyber crisis management plans referred to in Article 7(2a);

(ig) adopt recommendations on the basis of the results of Union level coordinated security risk assessments of critical supply chains referred to in Article 22 of Directive (EU) 2022/2555 to support Union entities in adopting effective and proportionate cybersecurity risk-management measures relating to supply chain security referred to in Article 5(1a), point (m);

(ih) develop guidelines for information sharing arrangements referred to in Article 19.

Article 11

Compliance

1. The IICB shall monitor the implementation of this Regulation and of adopted guidance documents, recommendations and calls for action by the Union ***entities***. Where the

IICB finds that Union ***entities*** have not effectively applied or implemented this Regulation or guidance documents, recommendations and calls for action issued under this Regulation, it may, without prejudice to the internal procedures of the relevant Union ***entity***:

(-a) request relevant and available documentation of the Union entity concerned;

(-aa) communicate a reasoned opinion to the Union entity concerned with observed gaps in the implementation of this Regulation;

(-ab) invite the Union entity concerned to provide a self-assessment on its reasoned opinion within a specified timeframe;

(-ac) provide, after consulting CERT-EU, guidance to the individual Union entity to bring its respective framework, cybersecurity risk-management measures, cybersecurity plans and reporting obligations in compliance with this Regulation within a specified period;

(a) issue a warning; where necessary in view of a compelling cybersecurity risk, the audience of the warning shall be restricted appropriately;

(b) ***request*** a relevant audit service to carry out an audit***;***

(ba) inform the Court of Auditors of the alleged non-compliance.

All warnings and recommendations shall be directed to the highest level of management of the Union entity concerned.

2. Where the small Union entities notify that they are unable to meet the deadlines set out in Articles 4(1) and 5(1), the IICB may, in exceptional cases, authorise their extension and set the deadlines for the compliance.

Chapter IV

CERT-EU

Article 12

CERT-EU mission and tasks

1. The mission of CERT-EU, the autonomous interinstitutional Cybersecurity Centre for all Union ***entities***, shall be to contribute to the security of the unclassified ***ICT***

environment of all Union ***entities and providing for them services that are analogous to CSIRTs established by the Member Sates under Directive (EU) 2022/2555, in particular*** by advising them on cybersecurity, by helping them to prevent, detect, ***handle,*** mitigate***,*** respond to ***and recover from*** incidents and by acting as their cybersecurity information exchange and incident response coordination hub.

2. CERT-EU shall perform the following tasks for the Union ***entities***:

(a) support them with the implementation of this Regulation and contribute to the coordination of the application of this Regulation through the measures listed in Article 13***(***1***)*** or through ad-hoc reports requested by the IICB;

(b) support them with a package of cybersecurity services described in its service catalogue ('baseline services');

(ba) operate for Union entities who do not have capacity to do it on on their own a broad-spectrum Security Operations Centre (SOC) which monitors networks, including first-line 24/7 monitoring for high-severity threats;

(c) maintain a network of peers and partners to support the services as outlined in Articles 16 and 17;

(d) raise to the attention of the IICB any issue relating to the implementation of this Regulation and of the implementation of ***Article 13 and submit proposals for recommendations***;

(e) report ***to the Union entities*** on the ***relevant*** cyber threats ▌ and contribute to the ***Union*** cyber situational awareness***, taking into account the opinion of ENISA, and submit such reports to the IICB, to the CSIRT network referred to in Article 15 of Directive (EU) 2022/2555 and to the EU Intelligence and Situation Centre (EU-INTCEN);***

(ea) act as the designated coordinator for the Union entities, for the purpose of coordinated vulnerability disclosure to the European vulnerability database referred to in Article 12 of Directive (EU) 2022/2555;

(eb) propose to the IICB, after consulting ENISA, the security criteria, a list of possible KPIs, and scale in the cybersecurity frameworks used by the Union entities;

(ec) propose to the IICB and prioritise, after consulting ENISA, the cybersecurity domains and the cybersecurity measures that Union entities are to take into account in their cybersecurity framework;

(ed) provide the Union entities with one or more cybersecurity maturity models, which are to be used in their cybersecurity frameworks and which reflect their size and the cybersecurity domains that they use;

(ee) provide services that support, with a high level of transparency and reliability, information exchanges, in particular with regard to the Union entities' notifications to CERT-EU;

(ef) conduct regular risk analysis of the interconnectivity among the Union entities in support of the IICB tasks.

3. CERT-EU shall contribute to the Joint Cyber Unit, built in accordance with the Commission Recommendation of 23 June 2021, including in the following areas:

(a) preparedness, incident coordination, information exchange and crisis response at the technical level on cases linked to Union ***entities***;

(b) operational cooperation regarding the computer security incident response teams (CSIRTs) network, including on mutual assistance, and the broader cybersecurity community;

(ba) coordination of the management of major incidents and crises at operational level and regular exchange of relevant information among Member States and Union entities within the European cyber crises liaison organisation network (EU-CyCLONe);

(c) cyber threat intelligence, including situational awareness;

(ca) proactive scanning of network and information systems;

(d) on any topic requiring CERT-EU's technical cybersecurity expertise.

4. CERT-EU shall engage in structured cooperation with ***ENISA*** on capacity building, operational cooperation and long-term strategic analyses of cyber threats in accordance with Regulation (EU) 2019/881 ▌. ***CERT-EU may cooperate and exchange information with Europol's European Cybercrime Centre.***

5. CERT-EU may provide ***to the Union entities*** the following services not described in its service catalogue ('chargeable services'):

(a) services that support the cybersecurity of Union ***entities' ICT*** environment, other than those referred to in paragraph 2, on the basis of service level agreements and subject to available resources***, including, via its Security Operations Centre referred to in paragraph 2, point (ba), monitoring of the networks and first-line 24/7 monitoring for high-severity threats for larger Union entities***;

(b) services that support cybersecurity operations or projects of Union ***entities***, other than those to protect their ***ICT*** environment, 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 ***entities*** that cooperate closely with Union ***entities***, 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.

6. CERT-EU ***shall*** organise cybersecurity exercises or recommend participation in existing exercises, in close cooperation with ***ENISA*** whenever applicable, to test the level of cybersecurity of the Union ***entities on a regular basis***.

7. CERT-EU ***shall*** provide assistance to Union ***entities*** regarding incidents in classified ***ICT*** environments if it is explicitly requested to do so by the constituent concerned. ***The provisions and obligations on all Union entities set out in Chapter V shall not apply to incidents in classified ICT environments unless an individual Union entity explicitly and voluntarily apply them in order to seek actionable assistance from CERT-EU or otherwise contribute to situational awareness at Union level.***

7a. CERT-EU shall submit, under appropriate confidentiality conditions, a yearly report of its activities to the European Parliament. That report shall include relevant and precise information about the major incidents and the way they were dealt with.

7b. CERT-EU shall cooperate with the EDPS to support Union entities in incidents entailing a personal data breach as defined in Article 3, point (16), of Regulation (EU) 2018/1725.

7c. The processing of personal data carried out by CERT-EU under this Regulation shall be subject to Regulation (EU) 2018/1725.

7d. ***CERT-EU may provide assistance to Union entities regarding the implementation of appropriate cybersecurity cooperation between them in terms of cybersecurity knowledge, staff and ICT resources, and cybersecurity expertise.***

7e. ***CERT-EU shall inform the EDPS when addressing significant vulnerabilities, significant incidents or major incidents that have the potential to result in personal data breaches and/or in the breach of confidentiality of electronic communications.***

7f. ***CERT-EU shall inform the EDPS about preventive cybersecurity activities that would result in the collection of personal data.***

Article 13

Guidance documents, recommendations and calls for action

1. CERT-EU shall support the implementation of this Regulation by issuing:

   (a) calls for action describing urgent security measures that Union ***entities*** are urged to take within a set timeframe;

   (b) proposals to the IICB for guidance documents addressed to all or a subset of the Union ***entities***;

   (c) proposals to the IICB for recommendations addressed to individual ***or all Union entities***.

2. Guidance documents and recommendations may include:

   (a) modalities for or improvements to cybersecurity risk management and ▌ cybersecurity ***risk-management measures***;

   (b) ***arrangements*** for ***cybersecurity*** maturity assessments and cybersecurity plans; and

   (c) where appropriate, the use of common technology, ***open-source*** architecture and associated best practices with the aim of achieving interoperability and common standards***;***

   (ca) where appropriate, facilitate the common purchasing of relevant ICT services and ICT products.

▌

Article 14

Head of CERT-EU

The Commission, after obtaining the approval of a majority of two thirds of the IICB members, shall appoint the head of CERT-EU. The IICB shall be consulted at all stages of the procedure prior to the appointment of the head of CERT-EU, in particular in drafting vacancy notices, examining applications and appointing selection boards in relation to that post. The final list of candidates shall include at least one man and one woman.

The head of CERT-EU shall ▌ submit reports ***at least once a year*** to the IICB and the IICB Chair on the ***activities and*** performance of CERT-EU ***during the reference period***, ***including on the*** 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 ▌ . ***Those reports shall include the work programme for the next period, financial planning of revenue and expenditure, including staffing, planned updates of CERT-EU's service catalogue and an assessment of the expected impact that such updates may have in terms of financial and human resources.***

The head of CERT-EU shall also submit, ad-hoc reports to the IICB upon its request.

Article 15

Financial and staffing matters

1. ***CERT-EU is an autonomous interinstitutional service provider for all Union entities, integrated into the administrative structure of a Commission Directorate-General in order to benefit from the Commission's administrative, financial, management and accounting support structures.*** The Commission ▌ shall ***inform the IICB about the administrative location*** of CERT-EU ***and any changes thereto***. ***This approach is to be evaluated on a regular basis, in order to allow appropriate action to be taken, including the possible establishment of CERT-EU as a Union office.***

1a. All decisions related to staffing and budget allocation of the CERT-EU shall be submitted to the formal approval of the IICB.

2. For the application of administrative and financial procedures, the head of CERT-EU shall act under the authority of the Commission ***under the supervision of the IICB***.

3. CERT-EU tasks and activities, including services provided by CERT-EU pursuant to Article 12(2), (3), (4), (6), and Article 13(1) to Union ***entities*** financed from the heading of the multiannual financial framework dedicated to European public administration, shall be funded through a distinct budget line of the Commission budget. CERT-EU earmarked posts shall be detailed in a footnote to the Commission establishment plan.

4. Union ***entities*** other than those referred to in paragraph 3 shall make an annual financial contribution to CERT-EU to cover the services provided by CERT-EU pursuant to that paragraph 3. The respective contributions shall be based on orientations given by the IICB and agreed between each entity and CERT-EU in service level agreements. The contributions shall represent a fair and proportionate share of the total costs of services provided. They shall be received by the distinct budget line referred to in paragraph 3 as assigned revenue as provided for in Article 21(3), point (c) of Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council[9].

5. The costs of the tasks defined in Article 12(5) shall be recovered from the Union ***entities*** receiving the CERT-EU services. The revenues shall be assigned to the budget lines supporting the costs.

Article 16

Cooperation of CERT-EU with Member State counterparts

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 ***(EU) 2022/2555***, on cyber threats, vulnerabilities***,*** incidents, ***near misses,*** possible countermeasures ***as well as***

[9] 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).

best practices and on all matters relevant for improving the protection of the ***ICT*** environments of Union ***entities***, including through the CSIRTs network referred to in Article ***15*** of Directive ***(EU) 2022/2555***. ***CERT-EU shall support the Commission in the EU-CyCLONe referred to in Article 16 of Directive (EU) 2022/2555 on coordinated management of major incidents and crises.***

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 ***authorisation*** of the ▌ constituent ***affected, provided that personal data is protected in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council***[10]. CERT-EU may only exchange incident-specific information which reveals the identity of the target of the cybersecurity incident with the ***authorisation*** of the ▌ constituent ***affected and in compliance with Regulation (EU) 2016/679***.

Article 17

Cooperation of CERT-EU with non-Member State counterparts

1. CERT-EU may cooperate with non-Member State counterparts ***that are subject to Union cybersecurity requirements or requirements of similar nature,*** 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.

2. CERT-EU may cooperate with other partners, such as commercial entities ***(including industry sector-specific entities)***, international organisations, non-European Union national entities or individual experts, to gather information on general and specific cyber threats***, near misses***, vulnerabilities and possible countermeasures. For wider cooperation with such partners, CERT-EU shall seek prior approval from the IICB.

---

[10] ***Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).***

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 analysis.

Chapter V

COOPERATION AND REPORTING OBLIGATIONS

Article 18

Information handling

1. CERT-EU and Union ***entities*** shall respect the obligation of professional secrecy in accordance with Article 339 of the Treaty on the Functioning of the European Union or equivalent applicable frameworks.

2. The provisions of Regulation (EC) No 1049/2001 of the European Parliament and the Council[11] shall apply with regard to requests for public access to documents held by CERT-EU, including the obligation under that Regulation to consult other Union ***entities, or, where relevant, Member States,*** whenever a request concerns their documents.

3. The processing of personal data carried out under this Regulation shall be subject to Regulation (EU) 2018/1725 ▌.

Any processing, exchange, collection or retention of personal data by CERT-EU, the IICB and Union entities shall be limited to processing, exchange, collection or retention that is strictly necessary and shall be carried out for the sole purpose of fulfilling their respective obligations under this Regulation.

3a. The Commission shall, by ... [one year after the date of entry into force of this Regulation], adopt a delegated act in accordance with Article 24a to specify which personal data processing activities are permitted under this Regulation, including the purpose of the processing, the categories of personal data, the categories of data subjects, the conditions for data processing, maximum retention periods, the

---

11 Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43).

definition of the data controllers and processors and recipients in the case of transmission.

The delegated act referred to in the first subparagraph shall limit processing activities to those that are strictly necessary and shall require that such processing activities be as targeted as possible and do not include the indiscriminate retention of traffic or content data.

The Commission shall amend the delegated act referred to in the first subparagraph where it identifies significant changes with regard to the necessity or specific purposes, or to the entities involved in the processing of personal data for the purposes of this Regulation.

4. The handling of information by CERT-EU and its Union ***entities*** shall be in line with the rules laid down in [proposed Regulation on information security]. ***When cooperating with other counterparts equivalent information handling rules shall be used by the CERT-EU.***

5. Any contacts with CERT-EU initiated or sought by national security and intelligence services shall be communicated to the Commission's Security Directorate***, Europol*** and the chair of the IICB without undue delay.

5a. Information on the completion of security plans by the Union entities shall be shared with the discharge authorities.

5b. Guidance documents and recommendations, and calls for actions issued by the IICB shall be shared with the discharge authorities.

Article 19

Cybersecurity information sharing ***arrangements and*** obligations

-1. Union entities may voluntarily notify and provide information to CERT-EU on cyber threats, incidents, near misses and vulnerabilities that affect them. CERT-EU shall ensure that effective measures are adopted to ensure the confidentiality and appropriate protection of the information provided by the reporting Union entity. CERT-EU shall ensure that efficient means of communication are available for the purpose of facilitating information sharing with the Union entities. When processing notifications, CERT-EU may prioritise the processing of mandatory

notifications over voluntary notifications. Voluntary notification shall not result in the imposition of any additional obligations upon the reporting Union entity to which it would not have been subject had it not submitted the notification.

1. To enable CERT-EU ***effectively perform its mission and tasks laid down in Article 12 of this Regulation, in particular*** to coordinate vulnerability management ▌, it may request Union ***entities*** to provide it with information from their respective ***ICT*** system inventories that is relevant for ▌ CERT-EU support. The requested ***Union entity may*** transmit the requested information, and any subsequent updates thereto, without undue delay.

Without prejudice to Regulation (EU) 2018/1725, any sharing of data between CERT-EU and Union entities shall be carried out in line with the principles of clear safeguards for specific use-cases and shall use mutual legal assistance treaties and other agreements, in order to ensure a high level of protection for rights when processing requests for cross-border access to data.

▌

3. CERT-EU may only exchange incident-specific information which reveals the identity of the Union ***entity*** affected by the incident with the consent of that entity. CERT-EU may only exchange incident-specific information which reveals the identity of the target of the cybersecurity incident with the consent of the entity affected by the incident. ***In view of its scrutiny tasks, the European Parliament may request such information without the consent of the Union entity concerned. Where the European Parliament requests the information without the consent of the entity concerned, its deliberations shall not be held in public and all relevant documents shall be considered only on a need-to-know basis.***

4. The ***cybersecurity information*** sharing ***arrangements and*** obligations shall not extend to EU Classified Information (EUCI) and to information that a Union ***entity*** has received from a Member State Security or Intelligence Service or law enforcement agency***, unless the Member State Security or Intelligence Service or law enforcement agency concerned allow that information to*** be shared with CERT-EU.

Article 20

Reporting obligations

1. All Union ***entities*** shall ***report*** to CERT-EU ***in accordance with paragraph 1d any incident that has a significant impact. An incident shall be considered to be significant if:***

(a) it has caused or is capable of causing severe operational disruption of the service or financial losses for the entity concerned;

(b) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

1a. The Union entities shall notify, inter alia, any information enabling the CERT-EU to determine any cross-entities impact, impact on the hosting Member State or cross-border impact following a significant incident. The mere act of notification shall not render the notifying Union entity subject to increased liability.

1b. Where applicable, Union entities shall notify, without undue delay, to the users of the network and information systems affected, or other components of the ICT environment, that are potentially affected by a significant incident or a significant cyber threat of any measures or remedies that can be taken in response to the incident or threat. Where appropriate, Union entities shall inform users of the threat itself.

1c. Where a significant incident or significant cyber threat affects a network and information system, or a component of a Union entity's ICT environment that is knowingly connected with another Union entity's ICT environment, CERT-EU shall notify, without undue delay, the Union entity affected.

1d. All Union entities shall submit to CERT-EU:

(a) without undue delay and in any event within 24 hours of becoming aware of the significant incident, an early warning, which, where applicable, shall indicate whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-entity or a cross-border impact;

(b) without undue delay and in any event within 72 hours of becoming aware of the significant incident, an incident report, which, where applicable, shall update the information referred to in point (a) and indicate an initial

assessment of the significant incident, its severity and impact, as well as, where available, the indicators of compromise;

(c) upon the request of CERT-EU, an intermediate report on relevant status updates.

2. The Union ***entities*** shall further ***submit*** to CERT-EU ***a final report, not later than one month after the submission of the incident report, referred to in paragraph 1d, point (b). In cases of ongoing significant incidents at the time of the submission of the final report, a progress report at that time and a final report shall be transmitted within one month after the*** incident ***has been handled. The incident report*** shall include ***at least the following,*** if available:

(a) ***a detailed description of the incident, including its severity and impact***;

(b) ***the type of threat or root cause that is likely to have triggered the incident***;

(c) ***the mitigation measures that have been or are being carried out***;

(d) ***where applicable, the potential impact of the incident on other Union entities or cross-border impact***.

2a. In duly justified cases and in agreement with CERT-EU, the Union entity concerned may derogate from the deadline laid down in paragraph 2. The Union entity concerned shall provide a progress report by the deadline of the submission of a final report, if a derogation is agreed on.

2b. The Union entities, upon the request of CERT-EU shall without undue delay, provide CERT-EU 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.

3. CERT-EU shall submit to ENISA on a monthly basis a summary report including anonymised and aggregated data on significant ***incidents,*** cyber threats, ***incidents, near misses and*** vulnerabilities ▌ notified in accordance with paragraph ***1d of this Article and with Article 19(-1)***.

4. ***By ... [one year after the date of entry into force of the Regulation], the CERT-EU shall*** issue guidance documents or recommendations ***on the arrangements relating to,*** and ***the*** content of***, the reports. When preparing such guidance documents or***

recommendations, the CERT-EU shall take into account the specifications made by any implementing acts adopted by the Commission specifying the type of information, the format and the procedure of a notification ***submitted pursuant to Article 23(11) of Directive (EU) 2022/2555***. CERT-EU shall disseminate the appropriate technical details to enable proactive detection, incident response or mitigating measures by Union ***entities***.

5. The ***reporting*** obligations shall not extend to EUCI and to information that a Union ***entity*** 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 CERT-EU.

Article 21

Incident response coordination and cooperation ▌

1. In acting as a cybersecurity information exchange and incident response coordination hub, CERT-EU shall facilitate information exchange with regards to cyber threats, vulnerabilities***, near misses*** and incidents among:

   (a) Union ***entities***;

   (b) the counterparts referred to in Articles 16 and 17.

2. CERT-EU shall facilitate coordination among Union ***entities*** on incident response, including:

   (a) contribution to consistent external communication;

   (b) mutual assistance;

   (c) optimal use of operational resources;

   (d) coordination with other crisis response mechanisms at Union level.

3. CERT-EU***, in cooperation with ENISA,*** shall support Union ***entities*** regarding situational awareness of cyber threats, vulnerabilities***, near misses*** and incidents***, as well as sharing the latest developments in the field of cybersecurity***.

4. ***By ... [one year after the date of entry into force of the Regulation],*** the IICB shall issue guidance on incident response coordination and cooperation for significant incidents. Where the criminal nature of an incident is suspected, ***IICB and*** CERT-EU

shall advise on how to report the incident to law enforcement authorities ***without undue delay***.

Article 22

Major ***incidents***

1. CERT-EU shall coordinate among ***the*** Union ***entities the handling of*** major ***incidents. In that respect,*** it shall maintain an inventory of ***the available*** technical expertise that would be needed for incident response in the event of such ***major incidents and assist the IICB in coordinating Union entities' cyber crisis management plans for major incidents referred to in Article 7(2a)***.

2. The Union ***entities*** shall contribute to the inventory of technical expertise by providing an annually updated list of experts available within their respective organisations detailing their specific technical skills.

3. With the approval of the ▌ Union ***entities concerned***, CERT-EU may also call on experts from the list referred to in paragraph 2 for contributing to the response to a major ***incident*** in a Member State, in line with the ▌operating procedures ***of EU CyCLONe***. ***Specific rules on access to and use of technical experts from Union entities shall be approved by IICB at the proposal of CERT-EU***.

Chapter VI

FINAL PROVISIONS

Article 23

Initial budgetary ***arrangements***

1. In its proposal for the first budget to be adopted after ... [the date of entry into force of this Regulation], the Commission shall take into account the increased budgeting and staffing needs of all Union entities, in particular those of the small Union entities, that are associated with the obligations arising from this Regulation.

2. In order to ensure proper and stable functioning of CERT-EU, the Commission ***may*** propose the reallocation of staff and financial resources ▌to the Commission budget ***for use in CERT-EU operations from the ICT budgets of certain Union entities on***

the basis of clear criteria and without prejudice to their cybersecurity. The reallocation shall be effective at the same time as the first budget adopted following the entry into force of this Regulation.

Article 24

Review

1. The IICB, with the assistance of CERT-EU shall ▌report***, at least once a year,*** to the Commission on the implementation of this Regulation. The IICB may also make recommendations to the Commission to propose amendments to this Regulation.

2. The Commission shall ***evaluate and*** report on the implementation of this Regulation ***and on the experience gained at a strategic and operational level*** to the European Parliament and the Council ***by ... [36*** months after the ***date of*** entry into force of this Regulation***]*** and every ***two*** years thereafter.

2a. The reports referred to in paragraph 2 of this Article shall evaluate, taking into account Article 15(1a), the possibility of setting up CERT-EU as a Union office.

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.

Article 24a

Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The power to adopt delegated acts referred to in Article 18(3a) shall be conferred on the Commission for an indeterminate period of time from ... [one day after the date of entry into force of this Regulation].

3. The delegation of power referred to in Article 18(3a) 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 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.

4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

5. A delegated act adopted pursuant to Article 18(3a) 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 25

Entry into force

This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at ...,

For the European Parliament	*For the Council*
The President	*The President*

I

EXPLANATORY STATEMENT

BACKGROUND

In its proposal on laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies (EUIBAs) of the Union, the Commission has set out measures for all Union entities to establish a framework for common cybersecurity rules and measures to improve their resilience and incident response capabilities. It is the first piece of Union legislation that focuses on the cybersecurity of the EUIBAs.

The aim of the proposal is to improve the resilience and incidence response capabilities of the Union entities and to extend the mandate and funding of CERT-EU, which will be renamed from ‘Computer Emergency Response Team' to ‘Cybersecurity Centre'. The proposal also establishes an Interinstitutional Cybersecurity Board (IICB), which tasks are to monitor the implementation of the Regulation by the EUIBAs and supervise the implementation of general priorities and objectives by CERT-EU.

RAPPORTEUR

The rapporteur welcomes the Commission’s proposal and agrees with the choice for a Regulation as the right instrument to address the increasing trend of cyber threats as, the number of significant incidents affecting EUIBAs authored by advanced persistent threat (APT) actors, has surged dramatically from 2019 to 2021. Therefore, cybersecurity issues should be paid more attention to and appropriate budget should be dedicated to it.

She is of the opinion that this proposal is essential to improve the resilience and protection of the public administration of the EU considering the increasing number of cybersecurity threats that are becoming more sophisticated. In this regard, interinstitutional cooperation is valuable for detecting, preventing, monitoring and responding to cyber threats and risks. EUIBAs to develop their cybersecurity measures and responses to cyber threats and potential attacks. A common approach is therefore necessary.

The rapporteur is of the opinion that EU institutions, bodies and agencies should be provided with adequate resources to face the challenges of increased cybersecurity threats. In particular, knowledge and skills in the field of cybersecurity should be safeguarded in the EUIBAs.

The proposal addresses the issue of human resources by centralizing resources to CERT-EU. The proposed centralized model is intended to improve the recruitment of experts into the EUIBAs. The rapporteur welcomes the strengthening of the mandate of CERT-EU and deems it necessary to provide it with the resources needed to fulfil it and its structure should be carefully considered in the future.

The EUIBAs vary considerably in size and in their role. Some of them have significant international networks. Therefore, the rapporteur highlights that a sufficient level of flexibility and a risk-based approach should be allowed for them to carry out their tasks. At the same time, a uniform approach for tackling cybersecurity threats should be found as all EUIBAs are interconnected and there should be no weak link in the chain.

1.3.2023

OPINION OF THE COMMITTEE ON CIVIL LIBERTIES, JUSTICE AND HOME 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 (*): Tomas Tobé

(*) Associated committee – Rule 57 of the Rules of Procedures

AMENDMENTS

The Committee on Civil Liberties, Justice and Home 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 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	(4) The Union institutions, bodies and agencies ***have been and*** 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.	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.

Amendment 2

Proposal for a regulation
Recital 5

Text proposed by the Commission	*Amendment*
(5) The Directive [proposal NIS 2] on measures for a high common level of cybersecurity across the Union aims to further improve the cybersecurity resilience and incident response capacities of public and private entities, national competent authorities and bodies as well as the Union as a whole. It is therefore necessary that Union institutions, bodies and agencies follow suit by ensuring rules that are consistent with the Directive [proposal NIS 2] and mirror its level of ambition.	(5) The Directive [proposal NIS 2] on measures for a high common level of cybersecurity across the Union aims to further improve the cybersecurity resilience and incident response capacities of public and private entities, national competent authorities and bodies as well as the Union as a whole. It is therefore necessary that Union institutions, bodies and agencies follow suit by ensuring rules that are consistent with the Directive [proposal NIS 2] and mirror its level of ambition. ***Security requirements should be at least equal to, or higher than, the minimum security requirements of the entities covered by Directive (EU) 2022/2555.***

Amendment 3

Proposal for a regulation
Recital 6 a (new)

Text proposed by the Commission	*Amendment*
	(6a) The Union institutions, bodies, offices and agencies should be provided with adequate means and tools by means of which to strengthen their cyber resilience. It is essential, therefore, to ensure that appropriate coordination

	mechanisms are in place for decision-making to be done in an efficient and effective manner.

Amendment 4

Proposal for a regulation
Recital 22

Text proposed by the Commission	*Amendment*
(22) All personal data processed under this Regulation should be processed in accordance with data protection legislation including Regulation (EU) 2018/1725 of the European Parliament and of the Council**.**[7]	(22) All personal data processed under this Regulation should be processed in accordance with ***Union*** data protection legislation including Regulation (EU) 2018/1725 of the European Parliament and of the Council[7]**.** ***This Regulation should not affect the application of Union law governing the processing of personal data, including the tasks conferred on and powers of the EDPS. CERT-EU and the IICB should work in close cooperation with the EPDS and staff specialised in data protection in Union institutions, bodies, offices and agencies to ensure full compliance with Union data protection law.***
[7] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).	[7] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

Amendment 5

Proposal for a regulation
Recital 22 a (new)

Text proposed by the Commission	*Amendment*
	(22a) Cybersecurity systems and services involved in the prevention, detection and response to cyber threats should comply with data protection and privacy law and should take relevant technical and organisational safeguarding measures to ensure that such compliance is achieved in an accountable way.

Amendment 6

Proposal for a regulation
Recital 23

Text proposed by the Commission	*Amendment*
(23) The handling of information by CERT-EU and the Union institutions, bodies and agencies should be in line with ***the*** rules laid down in Regulation [proposed Regulation on information security]. To ensure coordination on security matters, any contacts with CERT-EU initiated or sought by national security and intelligence services should be communicated to the Commission's Security Directorate and the chair of the IICB without undue delay.	(23) The handling of information by CERT-EU and the Union institutions, bodies and agencies should be in line with ***Union*** rules ***on information security, in particular those*** laid down in Regulation [proposed Regulation on information security]. To ensure coordination on security matters, any contacts with CERT-EU initiated or sought by national security and intelligence services should be communicated to the Commission's Security Directorate and the chair of the IICB without undue delay.

Amendment 7

Proposal for a regulation
Recital 25 a (new)

Text proposed by the Commission	*Amendment*
	(25a) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 and delivered an opinion on 17 May 2022,

Amendment 8

Proposal for a regulation
Article 4 – paragraph 5

Text proposed by the Commission	*Amendment*
5. Each Union institution, body and agency shall appoint a Local Cybersecurity Officer or an equivalent function who shall act as its single point of contact regarding all aspects of cybersecurity.	5. Each Union institution, body and agency shall appoint a Local Cybersecurity Officer or an equivalent function who shall act as its single point of contact regarding all aspects of cybersecurity. ***The Local Cybersecurity Officer shall cooperate with the data protection officer designated in accordance with Article 43 of Regulation (EU) 2018/1725 when dealing with overlapping activities, such as applying data protection by design and by default to cybersecurity measures and selecting cybersecurity measures that involve protection of personal data, integrated risk management and integrated security incident handling.***

Amendment 9

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 10

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

Text proposed by the Commission	*Amendment*
	(kb) the European Union Agency for Law Enforcement Cooperation.

Amendment 11

Proposal for a regulation
Article 12 – paragraph 2 – point e a (new)

Text proposed by the Commission	*Amendment*
	(ea) inform the European Data Protection Supervisor of any indication of an infringement by an Union institution, body, office or agency of the obligations laid down in this Regulation which comprises an unlawful processing of personal data;

Amendment 12

Proposal for a regulation
Article 12 – paragraph 2 – point e b (new)

Text proposed by the Commission	*Amendment*
	(eb) work in close cooperation with the European Data Protection Supervisor in the resolution of incidents resulting in personal data breaches or in breaches of the confidentiality of electronic communication.

Amendment 13

Proposal for a regulation
Article 12 – paragraph 7 a (new)

Text proposed by the Commission	*Amendment*
	7a. CERT-EU shall inform the European Data Protection Supervisor when addressing significant vulnerabilities, significant incidents or major attacks that have the potential to result in personal data breaches or in breaches of the confidentiality of electronic communication.

Amendment 14

Proposal for a regulation
Article 18 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The provisions of Regulation (EC) No 1049/2001 of the European Parliament and the Council[9] shall apply with regard to requests for public access to documents held by CERT-EU, including the obligation under that Regulation to consult other Union institutions, bodies and agencies whenever a request concerns their documents.	2. The provisions of Regulation (EC) No 1049/2001 of the European Parliament and the Council[9] shall apply with regard to requests for public access to documents held by CERT-EU, including the obligation under that Regulation to consult other Union institutions, bodies and agencies***, or, where relevant, Member States,*** whenever a request concerns their documents.
[9] Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43).	[9] Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43).

Amendment 15

Proposal for a regulation
Article 18 – paragraph 3 – subparagraph 1 a (new)

Text proposed by the Commission	*Amendment*
	Any processing, exchange, collection or retention of personal data by CERT-EU, the IICB and Union institutions, bodies, offices and agencies shall be limited to processing, exchange, collection or retention that is strictly necessary and shall be carried out for the sole purpose of fulfilling their respective obligations under this Regulation.

Amendment 16

Proposal for a regulation
Article 18 – paragraph 3 a (new)

Text proposed by the Commission	*Amendment*
	3a. The Commission shall, by ... [1 year after the date of entry into force of this Regulation], adopt a delegated act to specify which personal data processing activities are permitted under this Regulation, including the purpose of the processing, the categories of personal data, the categories of data subjects, the conditions for data processing, maximum retention periods, the definition of the data controllers and processors, and recipients in the case of transmission.
	The delegated act referred to in the first subparagraph shall limit processing activities to those that are strictly necessary and shall require that such processing activities be as targeted as possible and do not include the indiscriminate retention of traffic or content data.
	The Commission shall amend the delegated act referred to in the first subparagraph where it identifies significant changes with regard to the necessity or specific purposes, or to the entities involved in, the processing personal data for the purposes of this Regulation.

Amendment 17

Proposal for a regulation
Article 18 – paragraph 4

Text proposed by the Commission	*Amendment*
4. The handling of information by CERT-EU and its Union institutions, bodies and agencies shall be in line with ***the*** rules laid down in [proposed Regulation on information security].	4. The handling of information by CERT-EU and its Union institutions, bodies and agencies shall be in line with ***Union*** rules ***on information security, in particular those*** laid down in [proposed Regulation on information security].

Amendment 18

Proposal for a regulation
Article 18 – paragraph 5

Text proposed by the Commission	*Amendment*
5. Any contacts with CERT-EU initiated or sought by national security and intelligence services shall be communicated to the Commission's Security Directorate and the chair of the IICB without undue delay.	5. Any contacts with CERT-EU initiated or sought by national security and intelligence services shall be communicated to the Commission's Security Directorate***, Europol*** and the chair of the IICB without undue delay.

Amendment 19

Proposal for a regulation
Article 19 – title

Text proposed by the Commission	*Amendment*
Sharing ***obligations***	***Information*** Sharing

Amendment 20

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. ***In order for CERT-EU to carry out the tasks set out in Article 12, in particular in order*** to coordinate vulnerability management and incident response, Union institutions, bodies ***or*** agencies ***shall, upon a request by CERT-EU,*** provide ***CERT-EU*** with information from their respective ***ICT*** system inventories that is relevant for the CERT-EU support***, including any changes to their IT environment***. The requested ***entity*** shall transmit the requested information, and any subsequent updates thereto, without undue delay. ***Without prejudice to Regulation (EU) 2018/1725, any sharing of data between***

CERT-EU and Union institutions, bodies, offices or agencies shall be carried out in line with the principles of clear safeguards for specific use-cases and shall use mutual legal assistance treaties and other agreements, in order to ensure a high level of protection for rights when processing requests for cross-border access to data.

Amendment 21

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

Text proposed by the Commission	*Amendment*
	1a. Union institutions, bodies, offices and agencies may voluntarily provide CERT-EU with information on cyber threats and incidents, near misses and vulnerabilities affecting them. They may also request CERT-EU for further technical assistance and advice to combat cybersecurity incidents and major attacks. CERT-EU may prioritise the processing of mandatory notifications over voluntary notifications, save in the case of duly substantiated and urgent voluntary requests by Union institutions, bodies, offices and agencies.

Amendment 22

Proposal for a regulation
Article 19 – paragraph 3

Text proposed by the Commission	*Amendment*
3. CERT-EU may only exchange incident-specific information which reveals the identity of the Union institution, body or agency affected by the incident with the ***consent*** of that entity. CERT-EU may only exchange incident-specific information which reveals the identity of the target of	3. CERT-EU may only exchange incident-specific information which reveals the identity of the Union institution, body or agency affected by the incident with the ***authorisation*** of that entity. CERT-EU may only exchange incident-specific information which reveals the identity of

the cybersecurity incident with the ***consent*** of the entity affected by the incident.	the target of the cybersecurity incident with the ***authorization*** of the entity affected by the incident. ***Where necessary for the carrying out of its tasks, CERT-EU may exchange incident-specific information, including in the absence of authorisation on the part of the Union institution, body, office or agency affected by the incident. The Union institution, body, office or agency shall be notified of any such exchange of information in advance.***

Amendment 23

Proposal for a regulation
Article 19 – paragraph 4

Text proposed by the Commission	*Amendment*
4. The sharing obligations shall not extend to EU Classified Information (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 CERT-EU.	4. The sharing obligations shall not extend to EU Classified Information (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***, unless the Member State Security or Intelligence Service or law enforcement agency concerned allow that information to*** be shared with CERT-EU.

Amendment 24

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 be made public, subject to the relevant Union rules on***

	information security, in particular those laid down in [proposed Regulation on information security].

Amendment 25

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 ***CERT-EU***.	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***, unless the Member State Security or Intelligence Service or law enforcement agency concerned allow that information to*** be shared with ***CERT-EU***.

Amendment 26

Proposal for a regulation
Article 21 – paragraph 4

Text proposed by the Commission	*Amendment*
4. The IICB shall issue guidance on incident response coordination and cooperation for significant incidents. Where the criminal nature of an incident is suspected, CERT-EU shall ***advise on how to*** report the incident to law enforcement authorities.	4. The IICB shall issue guidance on incident response coordination and cooperation for significant incidents. Where the criminal nature of an incident is suspected, CERT-EU ***or the IICB*** shall report the incident to law enforcement authorities ***without undue delay***.

Amendment 27

Proposal for a regulation
Article 24 a (new)

Text proposed by the Commission	*Amendment*
	Article 24a

Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The power to adopt delegated acts referred to in Article 18(3a) shall be conferred on the Commission for an indeterminate period of time from ... [one day after the date of entry into force of this Regulation].

3. The delegation of power referred to in Article 18(3a) 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 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.

4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

5. A delegated act adopted pursuant to Article 18(3a) 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.

Amendment 28

Proposal for a regulation
Annex II – paragraph 1 – point 2 a (new)

Text proposed by the Commission	*Amendment*
	(2a) the use of encryption at rest, encryption in transit and end-to-end encryption where possible;

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	LIBE 4.4.2022
Associated committees - date announced in plenary	15.9.2022
Rapporteur for the opinion Date appointed	Tomas Tobé 12.12.2022
Discussed in committee	31.1.2023
Date adopted	1.3.2023
Result of final vote	+: 62 –: 0 0: 1
Members present for the final vote	Magdalena Adamowicz, Abir Al-Sahlani, Malik Azmani, Katarina Barley, Pietro Bartolo, Vladimír Bilčík, Vasile Blaga, Ioan-Rareş Bogdan, Karolin Braunsberger-Reinhold, Patrick Breyer, Saskia Bricmont, Patricia Chagnon, Caterina Chinnici, Clare Daly, Lena Düpont, Lucia Ďuriš Nicholsonová, Maria Grapini, Sylvie Guillaume, Andrzej Halicki, Evin Incir, Sophia in ‘t Veld, Patryk Jaki, Marina Kaljurand, Assita Kanko, Fabienne Keller, Łukasz Kohut, Moritz Körner, Alice Kuhnke, Jeroen Lenaers, Juan Fernando López Aguilar, Erik Marquardt, Nuno Melo, Maite Pagazaurtundúa, Karlo Ressler, Diana Riba i Giner, Birgit Sippel, Sara Skyttedal, Vincenzo Sofo, Tineke Strik, Ramona Strugariu, Annalisa Tardino, Tomas Tobé, Yana Toom, Milan Uhrík, Tom Vandendriessche, Jadwiga Wiśniewska
Substitutes present for the final vote	Susanna Ceccardi, Gwendoline Delbos-Corfield, Loucas Fourlas, Beata Kempa, Philippe Olivier, Dragoş Tudorache, Petar Vitanov, Tomáš Zdechovský
Substitutes under Rule 209(7) present for the final vote	Gheorghe Falcă, Jean-François Jalkh, Petra Kammerevert, Marisa Matias, Martina Michels, Ljudmila Novak, Stanislav Polčák, Mick Wallace, Bernhard Zimniok

FINAL VOTE BY ROLL CALL IN COMMITTEE ASKED FOR OPINION

62	+
ECR	Patryk Jaki, Assita Kanko, Beata Kempa, Vincenzo Sofo, Jadwiga Wiśniewska
ID	Susanna Ceccardi, Patricia Chagnon, Jean-François Jalkh, Philippe Olivier, Annalisa Tardino, Tom Vandendriessche, Bernhard Zimniok
PPE	Magdalena Adamowicz, Vladimír Bilčík, Vasile Blaga, Ioan-Rareş Bogdan, Karolin Braunsberger-Reinhold, Lena Düpont, Gheorghe Falcă, Loucas Fourlas, Andrzej Halicki, Jeroen Lenaers, Nuno Melo, Ljudmila Novak, Stanislav Polčák, Karlo Ressler, Sara Skyttedal, Tomas Tobé, Tomáš Zdechovský
Renew	Abir Al-Sahlani, Malik Azmani, Lucia Ďuriš Nicholsonová, Sophia in 't Veld, Fabienne Keller, Moritz Körner, Maite Pagazaurtundúa, Ramona Strugariu, Yana Toom, Dragoş Tudorache
S&D	Katarina Barley, Pietro Bartolo, Caterina Chinnici, Maria Grapini, Sylvie Guillaume, Evin Incir, Marina Kaljurand, Petra Kammerevert, Łukasz Kohut, Juan Fernando López Aguilar, Birgit Sippel, Petar Vitanov
The Left	Clare Daly, Marisa Matias, Martina Michels, Mick Wallace
Verts/ALE	Patrick Breyer, Saskia Bricmont, Gwendoline Delbos-Corfield, Alice Kuhnke, Erik Marquardt, Diana Riba i Giner, Tineke Strik

0	-

1	0
NI	Milan Uhrík

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

13.7.2022

OPINION OF THE COMMITTEE ON BUDGETS

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: Nils Ušakovs

SHORT JUSTIFICATION

Your rapporteur welcomes the Commission's proposal on laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies (EUIBAs) of the Union. He is of opinion that this proposal is necessary to improve the resilience and security of EU public administration in light of the increased number of cybersecurity threats more and more sophisticated. This is all the more accentuated by the current geopolitical context.

He believes that interinstitutional cooperation is key to adequately prevent, detect, monitor and respond to threats and risks. Each and every EUIBA, irrespective of its size, has a role to play and a responsibility to take in protecting the EUIBAs against cyberattacks, since a single, small loophole in one can put all the others at risk. The rapporteur therefore supports the idea of baseline cybersecurity measures. Moreover, he believes that interinstitutional cooperation, apart from enabling the EUIBAs to increase their IT cybersecurity and responses to cyberattacks, should also look at potential synergies in the working methods and communication channels, with the aim of reducing administrative burden, avoiding duplication of efforts and improving preparedness and protection.

Contrary to what the Commission proposes, the rapporteur is convinced that 42 posts instead of 21 posts are needed in order for CERT-EU to operate with fully-fledged and state of the art services. He disagrees with the Commission's proposal on compensating partially additional posts dedicated to CERT-EU by reducing the number of contracts agents.

The rapporteur advocates that, given its relative size and its request for additional posts as regards cybersecurity in its 2023 statement of estimates, the European Parliament should assign first 48 posts to CERT-EU in the first budget adopted following the entry into force of this Regulation. For the following three years, 14 of these posts will be reassigned yearly to the Parliament to leave at the end six posts permanently in CERT-EU. This gradual transfer back will allow for stability of staff and knowledge management. At the same time, the other relevant EUIBAs, after the first year, will assign posts gradually to CERT-EU. This will enable creating a pool of 42 new permanent staff in CERT-EU as from the onset.

The rapporteur proposes that the current mechanisms of service level agreements for chargeable services to be improved, as recommended the European Court of Auditors in its Special Report 05/2022[1] to ensure better cash flows management and reduce administrative work.

Finally, the rapporteur recommends that investments and posts dedicated to cybersecurity in the EUIBAs to be earmarked. This will allow identifying and sharing best practice and potential financing needs at EUIBAs level.

[1] Special report 05/2022: Cybersecurity of EU institutions, bodies and agencies : Level of preparedness overall not commensurate with the threats

AMENDMENTS

The Committee on Budgets 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 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 and agencies, ***including in the size of their human and financial resources,*** 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.

Justification

One cannot expect the same contribution from a small agency or body than from a Union institution.

Amendment 2

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	(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 level of cybersecurity***;*** in the longer term ***a target in the order*** of 10% should be ***pursued***.	information system concerned, taking into account the state of the art of such measures. Each Union institution, body and agency should aim to allocate adequate ***resources from*** its IT budget to improve its level of cybersecurity ***and to ensure at least a minimum level of cybersecurity corresponding to the risk assessment. The cost of ensuring cybersecurity depends on several factors such as size of the entity, need to ensure specific protections, attack surface and threat profile, and includes fixed costs and a variable portion. Due to the ever increasing threats,*** in the longer term ***up to*** of 10% ***of an entity's budget could be necessary to ensure an appropriate security level, as required by industry standards. In accordance with the recommendation of the European Data Protection Supervisor set out in its opinion 8/2022 of 17 May 2022, the minimum security requirements laid down in this Regulation*** should be ***equal to or higher than the minimum security requirements of the entities of NIS and NIS 2.0 proposals***.

Justification

According to industry standard, 10 % of the information, communications and technology (ICT) budget should be spent on cybersecurity. The IT budget should be commensurate to risks at each EUIBA's in line with their external and internal environments. In its Opinion 8/2022, the EDPS recommends adding in the proposal that its minimum security requirements should be at least equal or higher than the minimum security requirements of the entities of NIS and NIS 2.0 Proposal.

Amendment 3

Proposal for a regulation
Recital 8 a (new)

Text proposed by the Commission	*Amendment*
	(8a) In order to recover the costs of the chargeable services from the Union's institutions, bodies and agencies benefiting from these services, CERT-EU

should ensure that the service level agreements, from which more than 90 % of the CERT-EU 2020 budget derived from, do not create unnecessary administrative burden and are a useful tool to plan future cash flow revenues.

Justification

According to ECA Special Report 05/2022, service level agreements need to be renewed individually every year. This creates administrative burden and cash flow problems as CERT-EU does not have funds coming in at the same time from all SLAs. Agencies can terminate SLAs at any moment which can start a vicious circle where, due to lost revenue CERT-EU will have to scale back its services and cannot keep up with demand, prompting other EUIBAs to terminate their SLAs and move to private providers. Therefore, the current funding model is not ideal for ensuring a stable and optimal level of service.

Amendment 4

Proposal for a regulation
Recital 8 b (new)

Text proposed by the Commission	*Amendment*
	(8b) In order to be able to guarantee an effective cybersecurity framework and to provide for a high range of services to Union institutions, bodies and agencies, CERT-EU requires stable, highly qualified and specialised staff. In addition, to ensure the effective management of knowledge, a large share of the personnel assigned to CERT-EU should be permanent. Those staff should have access to continuous training programs.

Justification

42 additional permanent posts are to be allocated to CERT-EU to keep knowledge inside CERT-EU. Parliament should assign first 48 posts to CERT-EU in the first budget adopted following the entry into force of this Regulation. For the following three years, 14 of these posts will be reassigned yearly to Parliament, leaving six posts permanently in CERT-EU. At the same time, other relevant EUIBAs, after the first year, will assign posts gradually to CERT-EU. This mechanism will enable creating a pool of 42 permanent posts as from the onset, with appropriate access to training programs.

Amendment 5

Proposal for a regulation
Recital 8 c (new)

Text proposed by the Commission	*Amendment*
	(8c) In the current geopolitical context, it is essential that the confidentiality of data is at all times protected against cyber threats by specialised and operational teams.

Amendment 6

Proposal for a regulation
Recital 8 d (new)

Text proposed by the Commission	*Amendment*
	(8d) Prior to the allocation of additional staff resources, the Commission should conduct an analysis of the needs, taking into account the long-term perspective.

Amendment 7

Proposal for a regulation
Recital 10 a (new)

Text proposed by the Commission	*Amendment*
	(10a) Interinstitutional cooperation and trust is key to protecting, in an efficient and effective manner, the IT environment of the Union and thus its democratic voice. All the stakeholders concerned should always keep in mind increasing synergies, reducing administrative burden and avoiding duplication of efforts.

Justification

Several bodies and networks are involved in preparing guidance and collecting information on IT incidents, responses. etc. Cooperation between all these stakeholders is essential to avoid duplication of efforts, find synergies and ensure fast and effective communication flows

amongst them.

Amendment 8

Proposal for a regulation
Recital 10 b (new)

Text proposed by the Commission	*Amendment*
	(10b) To be consistent with the policy that the Union promotes vis-à-vis the Member States, the Union institutions, bodies, offices and agencies should renounce the use and development of software, such as Pegasus, that could infringe the right to privacy and the legal order of the Union;

Justification

In its report of 15 February 2022 "Preliminary Remarks on Modern Spyware", the EDPS invited Members States to renounce the use and development on European soil of software such as Pegasus which might affect the right to privacy, the democracy and the rule of law, and could therefore be incompatible with the democratic values and the legal order of the Union.

Amendment 9

Proposal for a regulation
Recital 11

Text proposed by the Commission	*Amendment*
(11) In May 2011, the Secretaries-General of the Union institutions and bodies decided to establish a pre-configuration team for a computer emergency response team for the Union's institutions, bodies and agencies (CERT-EU) supervised by an inter-institutional Steering Board. In July 2012, the Secretaries-General confirmed the practical arrangements and agreed to maintain CERT-EU as a permanent entity to continue to help improve the overall level	(11) In May 2011, the Secretaries-General of the Union institutions and bodies decided to establish a pre-configuration team for a computer emergency response team for the Union's institutions, bodies and agencies (CERT-EU) supervised by an inter-institutional Steering Board. In July 2012, the Secretaries-General confirmed the practical arrangements and agreed to maintain CERT-EU as a permanent entity to continue to help improve the overall level

of information technology security of the Union's institutions, bodies and agencies as an example of visible inter-institutional cooperation in cybersecurity. In September 2012, CERT-EU was established as a Taskforce of the European Commission with an interinstitutional mandate. In December 2017, the Union institutions and bodies concluded an interinstitutional arrangement on the organisation and operation of CERT-EU[3] . This arrangement should continue to evolve to support the implementation of this Regulation.	of information technology security of the Union's institutions, bodies and agencies as an example of visible inter-institutional cooperation in cybersecurity. In September 2012, CERT-EU was established as a ***permanent*** Taskforce of the European Commission with an interinstitutional mandate. In December 2017, the Union institutions and bodies concluded an interinstitutional arrangement on the organisation and operation of CERT-EU[3] . This ***interinstitutional*** arrangement should continue to evolve to ***be in line and*** support the implementation of this Regulation.
[3] OJ C 12, 13.1.2018, p. 1–11.	[3] OJ C 12, 13.1.2018, p. 1–11.

Justification

As per recital 11, CERT-EU was established as a permanent entity. The 2018 interinstitutional arrangement should be revised in order to take into account the breakdown of posts in Annex II a (new).

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	(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.	Agencies Network ***and enforce a gender balanced appointment procedure***. ***The IICB should require that all its members nominate a gender balanced representation.***

Justification

It is important to ensure that the gender balance principle is respected in the newly established IICB.

Amendment 11

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 and agencies, each Union institution, body and agency with IT expenditure should contribute a fair share to those services and tasks, ***either in posts, financial contributions or both, depending on the size of the institutions, bodies and agencies and the services and tasks provided***. Those contributions are without prejudice to the budgetary autonomy of the Union institutions, bodies and agencies.

Justification

Depending on the size of the Union institutions, bodies and agencies, contributions to CERT-EU could take the form of allocation of posts and financial contributions.

Amendment 12

Proposal for a regulation
Recital 24 a (new)

Text proposed by the Commission	*Amendment*
	(24a) All Union institutions, bodies and agencies should apply the gender equality and gender balance principles in their appointments to the CERT-EU as well as

in the allocation of their human resources concerning the IT sector and cybersecurity. Targeted training and adequate resources should be devoted to promoting the employment of women in the area of cybersecurity within all Union institutions, bodies and agencies in order to help to close the digital gender gap.

Justification

It is import to include the gender equality and gender balance principles in the regulation.

Amendment 13

Proposal for a regulation
Recital 25 a (new)

Text proposed by the Commission	*Amendment*
	(25a) In its conclusions of 23 May 2022 on the development of the European Union's cyber posture, the Council invited the relevant authorities and the Commission to reinforce the resilience of communications networks and infrastructures within the European Union. Therefore, it is important to strengthen the sovereignty and the resilience of the infrastructures and the control of connection, including the ones of the Union institutions, agencies and bodies;

Justification

In its Council conclusions on the development of the European Union's cyber posture dated 23 May 2022, the Council calls for strengthening the EU cyber resilience and its capacity to protect from cyberattacks.

Amendment 14

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 and agency shall have effective mechanisms in place to ensure that adequate ***resources from*** the IT budget ***are*** spent on cybersecurity ***bearing in mind the minimum percentage of IT budget to be spent on cybersecurity according to industry standards in order to protect effectively its IT environment***. ***Union institutions, bodies and agencies shall earmark resources assigned to CERT-EU in their budgets for more transparency.***

Justification

The Commission's proposal is unclear on what they mean by effective mechanisms and adequate percentage. At least, one criteria to assess an adequate percentage is the industry standard. Earmarking in the EUIBAs budget would create more transparency for investments in cybersecurity and identification of possible financial gaps and sharing best practices.

Amendment 15

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

Text proposed by the Commission	*Amendment*
	4a. Each Union institution, body and agency shall apply the gender equality and gender balance principles in their appointments to the CERT-EU as well as in the allocation of their human resources for cyber security. They shall devote targeted training and adequate resources to promoting the employment of women in the area of cybersecurity within all Union institutions, bodies and agencies in order to help to close the digital gender gap.

Justification

It is import to include the gender equality and gender balance principles in the regulation.

Amendment 16

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

Text proposed by the Commission	*Amendment*
	Members shall be nominated with due regard to the principle of gender balance.

Justification

It is important to include the gender equality and gender balance principles in the regulation.

Amendment 17

Proposal for a regulation
Article 12 – paragraph 7 a (new)

Text proposed by the Commission	*Amendment*
	7a. If the demand for chargeable services is higher than CERT-EU's available resources to provide for these services, CERT-EU shall prioritise demands based on a risk analysis taking into account the cybersecurity risk management of the requesting Union institutions, bodies and agencies, themselves impacted by the relative size of their financial and human resources.

Justification

EUIBAs should be prioritised based on their risks profile and taking into consideration the relative size of their financial and human resources.

Amendment 18

Proposal for a regulation
Article 14

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	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***, including***

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).	***on posts and external staff***, 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).

Justification

This amendment aims at clarifying that the report on the implementation of the budget should include the situation of posts and external staff in CERT-EU.

Amendment 19

Proposal for a regulation
Article 15 – paragraph 2

Text proposed by the Commission	*Amendment*
2. For the application of administrative and financial procedures, the Head of CERT-EU shall act under the authority of the Commission.	***deleted***

Amendment 20

Proposal for a regulation
Article 15 – paragraph 3

Text proposed by the Commission	*Amendment*
3. CERT-EU tasks and activities, including services provided by CERT-EU pursuant to Article 12(2), (3), (4), (6), and Article 13(1) to Union institutions, bodies and agencies financed from the heading of the multiannual financial framework dedicated to European public administration, shall be funded through a distinct budget line of the Commission budget. CERT-EU earmarked posts shall be detailed in a footnote to the Commission establishment plan.	3. CERT-EU tasks and activities, including services provided by CERT-EU pursuant to Article 12(2),(3), (4), (6), and Article 13(1) to Union institutions, bodies and agencies financed from the heading of the multiannual financial framework dedicated to European public administration, shall be funded through a distinct budget line of the Commission budget. CERT-EU earmarked posts shall be detailed in a footnote to the Commission establishment plan. ***The temporarily assigned posts shall be kept in the establishment plan of the donor institution during the temporary assignment and signalled with a footnote.***

This establishment plan shall be reviewed every 2,5 years.

Amendment 21

Proposal for a regulation
Article 15 – paragraph 3 a (new)

Text proposed by the Commission	*Amendment*
	3a. The transfer of a total of 42 posts by the relevant Union institutions, bodies and agencies as set out in Annex II a (new), without partial compensation from reduction of contract agents in CERT-EU, shall be without prejudice to the prerogatives of the Union's budgetary authority. The contributions shall represent a fair share which is in proportion to the respective share of permanent AD posts of the organisation and shall be made under due consideration of the principle of gender balance.

Justification

42 additional permanent posts are considered necessary to be assigned to CERT-EU. The breakdown of posts between relevant Union institutions, agencies and bodies should be agreed between the two arms of the budget authority during the inter-institutional negotiations for this proposal, subject to the prerogatives of the Union's budgetary authority. It is important to ensure that the gender balance principle is respected in the regulation.

Amendment 22

Proposal for a regulation
Article 23 – paragraph 1

Text proposed by the Commission	*Amendment*
The Commission shall propose the reallocation of ***staff and*** financial resources from relevant Union institutions, bodies and agencies to the Commission budget. ***The*** reallocation shall be effective at the same time as the first budget adopted following the entry into force of this	The Commission shall propose the reallocation of financial resources from relevant Union institutions, bodies and agencies to the Commission budget. ***This*** reallocation shall be effective at the same time as the first budget adopted following the entry into force of this Regulation.

Regulation.

Justification

The breakdown of posts assigned to CERT-EU is detailed in Annex II a (new).

Amendment 23

Proposal for a regulation
Annex II a (new)

Text proposed by the Commission

Amendment

Annex II a (new)

EUIBA/year	***Total staff***	***Posts assigned to CERT-EU at year N***	***Posts assigned to CERT-EU at N + 1***	***Posts assigned to CERT-EU at N + 2***	***Posts assigned to CERT-EU at N + 3***	***Posts permanently assigned to CERT-EU***
From previous year CERT-EU		***N/A***	***48***	***42***	***42***	
EP	***6.773***	***48***	***-14***	***-14***	***-14***	***6***
EC	***23.474***	***0***	***8***	***9***	***6***	***23***
Decentralised Agencies	***7.717***	***0***	***0***	***3***	***4***	***7***
CSL	***3.029***	***0***	***0***	***2***	***1***	***3***
EUCJ	***2.110***	***0***	***0***	***0***	***2***	***2***
EEAS	***1.753***	***0***	***0***	***0***	***1***	***1***
CoA	***873***	***0***	***0***	***0***	***0***	***0***
Executive agencies	***840***	***0***	***0***	***0***	***0***	***0***
EESC	***669***	***0***	***0***	***0***	***0***	***0***
JUs + Joint Technology Initiatives +European Institute of	***556***	***0***	***0***	***0***	***0***	***0***

Innovation and Technology						
CoR	***496***	***0***	***0***	***0***	***0***	***0***
EDPS	***84***	***0***	***0***	***0***	***0***	***0***
European Ombudsman	***73***	***0***	***0***	***0***	***0***	***0***
Total new staff		***48***	***42***	***42***	***42***	***42***

Justification

Breakdown of the 42 posts to be assigned to CERT-EU to ensure its proper and stable functioning.

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	BUDG 4.4.2022
Rapporteur for the opinion Date appointed	Nils Ušakovs 22.4.2022
Discussed in committee	20.6.2022 21.6.2022
Date adopted	12.7.2022
Result of final vote	+: 28 –: 0 0: 4
Members present for the final vote	Rasmus Andresen, Anna Bonfrisco, Olivier Chastel, Lefteris Christoforou, Andor Deli, José Manuel Fernandes, Eider Gardiazabal Rubial, Vlad Gheorghe, Francisco Guerreiro, Valérie Hayer, Eero Heinäluoma, Niclas Herbst, Monika Hohlmeier, Moritz Körner, Joachim Kuhs, Zbigniew Kuźmiuk, Janusz Lewandowski, Margarida Marques, Siegfried Mureşan, Victor Negrescu, Dimitrios Papadimoulis, Bogdan Rzońca, Nicolae Ştefănuţă, Nils Torvalds, Nils Ušakovs, Johan Van Overtveldt, Rainer Wieland
Substitutes present for the final vote	Damian Boeselager, Jan Olbrycht
Substitutes under Rule 209(7) present for the final vote	Alexander Bernhuber, Helmut Scholz, Birgit Sippel

FINAL VOTE BY ROLL CALL IN COMMITTEE ASKED FOR OPINION

28	+
ID	Anna Bonfrisco
NI	Andor Deli
PPE	Alexander Bernhuber, Lefteris Christoforou, José Manuel Fernandes, Niclas Herbst, Monika Hohlmeier, Janusz Lewandowski, Siegfried Mureşan, Jan Olbrycht, Rainer Wieland
Renew	Olivier Chastel, Vlad Gheorghe, Valérie Hayer, Moritz Körner, Nils Torvalds, Nicolae Ştefănuță
S&D	Eider Gardiazabal Rubial, Eero Heinäluoma, Margarida Marques, Victor Negrescu, Birgit Sippel, Nils Ušakovs
The Left	Dimitrios Papadimoulis, Helmut Scholz
Verts/ALE	Rasmus Andresen, Damian Boeselager, Francisco Guerreiro

0	-

4	0
ECR	Zbigniew Kuźmiuk, Bogdan Rzońca, Johan Van Overtveldt
ID	Joachim Kuhs

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

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

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 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.	(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, ***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,	(2) The cyber threat landscape faced by Union institutions, bodies***, offices*** and agencies is in constant evolution. The

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.

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	(4) The Union institutions, bodies***,***

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.	***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 level of cybersecurity***;*** in the ***longer term a target*** in the ***order of 10% should be pursued***.	(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 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, 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.	(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 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. 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.	(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 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	(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;***	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 cyber threat ***with the intention, opportunity and capability to cause a significant incident***;	(11) 'significant cyber threat' means a 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***	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***

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].	***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	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

cybersecurity.	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 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.	2. The senior management of each Union institution, body***, office*** and agency shall follow specific trainings on a regular 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 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.	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***, 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	(a) monitoring the implementation of

this Regulation by the Union institutions, bodies and agencies;	this Regulation by the Union institutions, bodies***, offices*** and agencies ***and making recommendations for achieving a common high level of cybersecurity***;

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 of the following:	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 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	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***.	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	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.	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 analysis.	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 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***	1. To ***perform its mission and tasks***

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.

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 CERT-EU.	***deleted***

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	(a) the removal of contractual barriers that limit information sharing from ***ICT*** service providers about incidents, vulnerabilities and cyber threats with

CERT-EU;	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

PROCEDURE – COMMITTEE RESPONSIBLE

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)
Date submitted to Parliament	22.3.2022
Committee responsible Date announced in plenary	ITRE 4.4.2022
Committees asked for opinions Date announced in plenary	BUDG LIBE AFCO 4.4.2022 4.4.2022 4.4.2022
Associated committees Date announced in plenary	LIBE 15.9.2022
Rapporteurs Date appointed	Henna Virkkunen 18.5.2022
Discussed in committee	26.10.2022
Date adopted	9.3.2023
Result of final vote	+: 58 –: 0 0: 0
Members present for the final vote	Nicola Beer, Hildegard Bentele, Tom Berendsen, Vasile Blaga, Michael Bloss, Marc Botenga, Martin Buschmann, Cristian-Silviu Buşoi, Jerzy Buzek, Ignazio Corrao, Beatrice Covassi, Ciarán Cuffe, Josianne Cutajar, Nicola Danti, Christian Ehler, Valter Flego, Niels Fuglsang, Lina Gálvez Muñoz, Claudia Gamon, Jens Geier, Nicolás González Casares, Bart Groothuis, Christophe Grudler, Henrike Hahn, Robert Hajšel, Ivo Hristov, Romana Jerković, Seán Kelly, Łukasz Kohut, Miapetra Kumpula-Natri, Marisa Matias, Dan Nica, Angelika Niebler, Ville Niinistö, Johan Nissinen, Mauri Pekkarinen, Tsvetelina Penkova, Morten Petersen, Manuela Ripa, Robert Roos, Maria Spyraki, Riho Terras, Grzegorz Tobiszowski, Patrizia Toia, Pernille Weiss
Substitutes present for the final vote	Andrus Ansip, Pascal Arimont, Izaskun Bilbao Barandica, Franc Bogovič, Jakop G. Dalunde, Matthias Ecke, Cornelia Ernst, Jens Gieseke, Jutta Paulus, Marion Walsmann, Emma Wiesner
Substitutes under Rule 209(7) present for the final vote	Agnès Evren, Tilly Metz
Date tabled	10.3.2023

FINAL VOTE BY ROLL CALL IN COMMITTEE RESPONSIBLE

58	+
ECR	Johan Nissinen, Robert Roos, Grzegorz Tobiszowski
NI	Martin Buschmann
PPE	Pascal Arimont, Hildegard Bentele, Tom Berendsen, Vasile Blaga, Franc Bogovič, Cristian-Silviu Buşoi, Jerzy Buzek, Christian Ehler, Agnès Evren, Jens Gieseke, Seán Kelly, Angelika Niebler, Maria Spyraki, Riho Terras, Marion Walsmann, Pernille Weiss
Renew	Andrus Ansip, Nicola Beer, Izaskun Bilbao Barandica, Nicola Danti, Valter Flego, Claudia Gamon, Bart Groothuis, Christophe Grudler, Mauri Pekkarinen, Morten Petersen, Emma Wiesner
S&D	Beatrice Covassi, Josianne Cutajar, Matthias Ecke, Niels Fuglsang, Lina Gálvez Muñoz, Jens Geier, Nicolás González Casares, Robert Hajšel, Ivo Hristov, Romana Jerković, Łukasz Kohut, Miapetra Kumpula-Natri, Dan Nica, Tsvetelina Penkova, Patrizia Toia
The Left	Marc Botenga, Cornelia Ernst, Marisa Matias
Verts/ALE	Michael Bloss, Ignazio Corrao, Ciarán Cuffe, Jakop G. Dalunde, Henrike Hahn, Tilly Metz, Ville Niinistö, Jutta Paulus, Manuela Ripa

0	-

0	0

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