Council of the European Union

Brussels, 30 September 2022
(OR. en)

10097/3/22
REV 3

LIMITE

CYBER 211
TELECOM 266
INST 227
CSC 246
CSCI 81
INF 97
FIN 654
BUDGET 14
DATAPROTECT 188
CODEC 891

Interinstitutional File:
2022/0085(COD)

NOTE

From:	Presidency
To:	Delegations
No. prev. doc.:	7474/22 + ADD 1
Subject:	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 - revised Presidency compromise

Following discussions at the meeting of the Horizontal Working Party on Cyber Issues on 13 September 2022, as well as subsequent delegations' written comments[1], delegations will find in the Annex a revised Presidency compromise on the above legislative proposal.

The recent changes are indicated in bold and underlining/strikethrough. Other changes as compared to the Commission proposal are marked in bold or bold/strikethrough.

[1] WK 12554/2022.

ANNEX

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 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.

(2) The cyber threat landscape faced by Union **~~institutions, bodies and agencies~~ 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' ~~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 **~~titution, body or agency~~ entity**, 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'~~ Union entities'** 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. **Furthermore, Union entities handle large amount and often sensitive information from Member States, therefore incidents compromising the availability, authenticity, integrity or confidentiality of such data could negatively affect Member States as well. For this reason, the cybersecurity of the Union entities is of high importance for the Member States as well**.

(4) The Union **~~institutions, bodies and agencies~~ 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 **~~institutions, bodies and agencies of the~~** Union **entities** achieve a high common level of cybersecurity through **implementation of concrete cybersecurity measures, ~~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.

(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~~ entities** follow suit by ensuring rules that are consistent with the Directive [proposal NIS 2] and mirror its level of ambition.

(6) To reach a high common level of cybersecurity, it is necessary that each Union **~~institution, body and agency~~ entity** establishes an internal cybersecurity risk management, governance and control framework that ensures an effective and prudent management of all cybersecurity risks **~~and takes account of business continuity and crisis management~~**. **The framework should lay down cybersecurity policies, including procedures to assess the effectiveness of implemented cybersecurity measures. The framework should be based on an all-hazard approach reflecting the findings of the risk analysis, taking account of all the relevant technical, operational and organizational risks to the cybersecurity of the concerned Union entity.**

(6a) To manage the risks identified under the framework, each Union entity should ensure that appropriate and proportionate cybersecurity measures are taken. These should address the domains, including concrete cybersecurity measures set out in this Regulation to strengthen the cybersecurity of each Union entity, such as the use of encryption and secured communication systems within the organization and others.

(6b) The assets and risks identified in the framework as well as conclusions derived from regular maturity assessments should be reflected in cybersecurity plan established by each Union entity. The cybersecurity plan should include the adopted cybersecurity measures, with the aim to increase the overall cybersecurity of the concerned Union entity.

(6c) As ensuring cybersecurity is a continuous process, the suitability and effectiveness of all measures should be regularly revised in light of the changing risks, assets and maturity of the Union. The framework should be revised on a regular basis and at least every three years, while the cybersecurity plan should be revised at least every two years or following every revision of the maturity assessment or every revision of the framework.

(6d) Union entities should exchange relevant information on a regular basis, including with regard to relevant incidents and cyber threats, while ensuring the confidentiality and appropriate protection of the information provided by the reporting entity.

(6e) A clear mechanism to ensure proper exchange of information, coordination, and cooperation of the Union entities in case of major incidents should be implemented, including a clear identification of the roles and responsibilities of the of the involved Union entities. The above-mentioned information should be taken into account by the designated point of contact for the EU-CyCLONe, when sharing relevant information with the EU-CyCLONe as a contribution to the shared situational awareness.

(7) The differences between Union ~~**institutions, bodies and agencies**~~ **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 institutions, bodies and agencies or encroaching on their institutional autonomy.**~~ Thus, those ~~**institutions, bodies and agencies**~~ **Union entities** should establish their own frameworks for cybersecurity risk management, governance and control and cybersecurity plans, and adopt ~~**their own baselines and cybersecurity plans**~~ **respective cybersecurity measures. When implementing such measures, due account should be taken of synergies existing between Union entities, with the aim of proper management of resources and cost optimization.**

(8) In order to avoid imposing a disproportionate financial and administrative burden on Union ~~institutions, bodies and agencies~~ **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 ~~institution, body and agency~~ **entity** 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~~. **The maturity assessment should also assess whether the Union entity's cybersecurity spending is proportionate to the risks it faces.**

(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~~ **entity. The highest level of management should oversee the implementation of this Regulation, including establishment of the risk management, governance and control framework, cybersecurity plans, encompassing concrete cybersecurity measures.**

(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~~ **Cybersecurity** measures should form part of the cybersecurity ~~baseline~~ **plan** and be further specified in guidance documents or recommendations issued by CERT-EU. When defining measures and guidelines, due account should be taken of **the state of the art and, where applicable, relevant European and international standards, as well as** 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~~ **should** be required, under specific EU 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]. This ~~arrangement~~ **Regulation should provide a comprehensive set of rules on the organisation, functioning and operation** ~~should continue to evolve to support the implementation of this Regulation.~~ **of CERT-EU.**

~~(12) CERT-EU should be renamed from 'computer emergency response team' to 'Cybersecurity Centre' for the Union institutions, bodies and agencies, 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.~~

[2] OJ C 12, 13.1.2018, p. 1–11.

(13) Many cyberattacks are part of wider campaigns that target groups of Union ~~**institutions, bodies and agencies**~~ **entities** or communities of interest that include Union ~~**institutions, bodies and agencies**~~ **entities**. To enable proactive detection, incident response or mitigating measures, Union ~~**institutions, bodies and agencies**~~ **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, similar **cyber threats, vulnerabilities, near misses and** incidents in other Union ~~**institutions, bodies and agencies**~~ **entities**. Following the same approach as the one envisaged in Directive [proposal NIS 2], where **Union** entities become aware of a significant incident they should be required to submit an ~~**initial notification**~~ **early warning** to CERT-EU within 24 hours. Such information exchange should enable CERT-EU to disseminate the information to other Union ~~**institutions, bodies and agencies**~~ **entities**, 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**~~.

(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 mitigate the potential spread of significant incidents and 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 cyber resilience of individual entities and entire sectors. In that regard, this Regulation should include the reporting of incidents that, based on an initial assessment carried out by the Union entity, could cause severe operational disruption to the functioning of the Union entity or financial loss to the Union entity concerned 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 affected network and information systems, in particular their importance for the functioning of the Union entity, the severity and technical characteristics of a cyber threat and any underlying vulnerabilities that are being exploited as well as the Union entity's experience with similar incidents. Indicators such as the extent to which the functioning of the Union entity is affected, the duration of an incident or the number of affected recipients could play an important role in identifying whether the operational disruption 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 **have the exclusive role to** facilitate a high common level of cybersecurity among Union ~~**institutions, bodies and agencies**~~ **entities** by monitoring the implementation of this Regulation by the Union ~~**institutions, bodies and agencies**~~ **entities** and by supervising implementation of general priorities and objectives by CERT-EU and providing strategic direction to CERT-EU. The IICB should ensure **therefore** representation of the institutions and include representatives of agencies and bodies through the Union Agencies Network. **The organisation and functioning of the IICB should be further regulated by its internal rules of procedures that may include further specification of regular meetings of the IICB, including annual gatherings of the strategic level where representatives of the highest level of management of each member of the IICB would allow for the IICB to have strategic discussion and provide strategic guidance of the IICB. Furthermore, the IICB may nominate an Executive Committee to assist in its work and to delegate some of its tasks and powers to it, especially in terms of tasks that requires specific expertise of its members, for instance the approval of the service catalogue and any subsequent updates to it, modalities for service level agreements or assessments of documents and reports submitted by the Union entities to the IICB according to this Regulation. The IICB should lay down the rules of procedures of the Executive Committee, including its tasks and powers.**

(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 ~~**institutions, bodies and agencies**~~ **entities** are urged to take within a set timeframe**. The IICB may instruct CERT-EU to issue, withdraw, or modify a proposal for guidance documents or recommendation, or a call for action.**

(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**~~ **entities** and other stakeholders as necessary. ~~**Where necessary, the IICB should issue non-binding warnings and recommend audits.**~~ **Where the IICB finds that the Union entities have not efficiently applied or implemented this Regulation, including the guidance documents, recommendations or calls for action issued under this Regulation, it may, without prejudice to the internal procedures of the relevant Union entity, proceed with concrete compliance measures. The system of compliance measures should be used with a progressive severity, meaning that when the IICB will need to adopt the compliance measures it should start with a warning as the least severe measure and if necessary escalate all the way to the most severe measure of issuing an advisory recommending temporary suspension of data flows to the concerned Union entity, which would be applied in exceptional cases of long-term, deliberate and/or serious non-compliance of the concerned entity with its obligation under this Regulation.**

(16a) The warning represents the least severe compliance measure addressing identified shortcomings of the Union entity and comprising recommendations to amend its cybersecurity documents, in a specified timeframe. The warning should be available to all Union entities, unless restricted appropriately in accordance with this Regulation.

(16b) The IICB may further recommend a relevant audit service to carry out an audit in each Union entity. In duly justified cases, for instance where the entity concerned cannot have an internal auditor perform an audit corresponding to the objectives and quality identified by the IICB, the IICB could request that such audits are carried out by a third-party audit service.

(16c) On the basis of the results of an audit carried out upon a recommendation or a request of the IICB, the IICB may further request the Union entity to bring the management, governance, and control of cybersecurity risks into compliance with the provisions of this Regulation.

(16d) As the Member States share with relevant Union entities information that may be of sensitive nature, the cybersecurity of the addressee of such information is crucial for the Member States. Therefore, in exceptional cases of long-term, deliberate, repetitive and/or serious non-fulfillment of the obligation of the Union entity, the IICB may issue as a last resort measure an advisory to all Member States and Union entities recommending temporary suspension of data flows the Union entity, that should be in place until the state of the cybersecurity of this entity is rectified.

(16e) To ensure the correct implementation of this Regulation by the European administration, the IICB should, if it considers that a continuous breach of this Regulation by a Union entity has been caused directly by the actions or omission of a member of its staff, including at the highest level of management, request the Union entity concerned to take appropriate actions against that staff member, in accordance with the Staff Regulations as well as other equivalent rules applicable in certain Union entities. These actions may include, for instance, disciplinary proceedings and, where appropriate, in the specific case of Union agencies, a request to the competent authority to take the necessary steps related to the possible removal from office of the person that could be responsible for the continuous breach of this Regulation.

(17) CERT-EU should have the mission to contribute to the security of the IT environment of all Union ~~institutions, bodies and agencies~~ **entities**. CERT-EU should act as the equivalent of the designated coordinator for the Union ~~institutions, bodies and agencies~~ **entities**, for the purpose of coordinated vulnerability disclosure to the European vulnerability registry as referred to in Article 6 of Directive [proposal NIS 2] **and should develop a policy on management of vulnerabilities, encompassing the promotion and facilitation of voluntary coordinated vulnerability disclosure.**

~~(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 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 institutions, bodies and agencies entities, 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 entities, CERT-EU should provide all the services.~~

(19) CERT-EU should also fulfill the role provided for it in Directive [proposal NIS 2] 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.

[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).

(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]. 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~~ **ENISA** on threat analysis and share its threat landscape report with the Agency on a regular basis.

~~(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) **The activities of CERT-EU and the information it deals with under this Regulation may involve processing of personal data.** 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.[6] **Where pursuant to this Regulation personal data is transmitted to recipients established in the Union other than Union entities, this should be done in accordance with Article 9 of Regulation (EU) 2018/1725.**

---

4 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15).

~~5 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 ~~institutions, bodies and agencies~~ **entities** 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.~~

(24) **This Regulation and the new tasks allocated to CERT-EU will have no effect on the total expenditures under the Multiannual Financial Framework.** As the services and tasks of CERT-EU are in the interest of all Union ~~institutions, bodies and agencies~~ **entities**, each Union ~~institution, body and agency~~ **entity** 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~~ **entities**. **All Union entities and their administrations should ensure the optimization of their resources at the current level and strengthen efficiency gains including by deepening inter-institutional cooperation in the area of cybersecurity. Therefore, a joint approach to pooling administrative expenditure should be given preference to individualized spending of Union entities.**

(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. **Furthermore, the European Court of Auditors is invited to evaluate the functioning of CERT-EU on a regular basis.**

HAVE ADOPTED THIS REGULATION:

Chapter I
GENERAL PROVISIONS

Article 1

Subject-matter

1. This Regulation **lays down measures that aim to achieve a high common level of cybersecurity within Union ~~institutions, bodies and agencies~~ entities**. ~~**lays down:**~~

2. To that end, this Regulation lays down:

(a) obligations on **each** Union ~~**institution, body and agency**~~ **entity** to establish **a** ~~**an internal**~~ cybersecurity risk management, governance and control framework;

(b) cybersecurity risk management ~~**and,**~~ reporting **and information sharing** obligations for Union ~~**institutions, bodies and agencies**~~ **entities**;

(c) rules on the organisation**, functioning** and operation of the ~~**Cybersecurity Centre**~~ **autonomous interinstitutional computer emergency response team** for the Union ~~**institutions, bodies and agencies**~~ **entities** (CERT-EU) and on the organisation**, functioning** and operation of the Interinstitutional Cybersecurity Board **(IICB)**;

(d) **rules relating to the monitoring of the implementation of this Regulation.**

Article 2

Scope

1. This Regulation applies to ~~**the management, governance and control of cybersecurity risks by**~~ all Union ~~**institutions, bodies and agencies**~~ **entities** and to ~~**the**~~ ~~**organisation and operation of**~~ CERT-EU and the **IICB** ~~**Interinstitutional Cybersecurity Board**~~.

2. **This Regulation applies without prejudice to the institutional autonomy** ~~**set out in**~~ **pursuant to the Treaties**.

3. **With the exception of Article 12 paragraph 7, this Regulation shall not apply to network and information systems handling EU Classified Information (EUCI).**

Article 3

Definitions

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

(1) 'Union ~~**institutions, bodies and agencies**~~ **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 **a** network and information system ~~**within the meaning of**~~ **as defined in** Article 4(1) of Directive [proposal NIS 2];

(3) 'security of network and information systems' means security of network and information systems ~~**within the meaning of**~~ **as defined in** Article 4(2) of Directive [proposal NIS 2];

(4) 'cybersecurity' means cybersecurity **~~within the meaning of Article 4(3) of Directive [proposal NIS 2]~~ 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 at the most senior administrative level **with decision capabilities**, taking account of the high-level governance arrangements in each Union **~~institution, body or agency~~ entity;**

(5a) 'near miss' means a near miss ~~within the meaning of~~ as defined in Article 4(4a) of Directive [proposal NIS 2]

(6) 'incident' means an incident **~~within the meaning of~~ as defined in** Article 4(5) of Directive [proposal NIS 2];

~~(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;~~

(8) 'major **incident** ~~attack~~' means any incident **which causes a level of disruption that exceeds a Union entity´s and CERT-EU´s capacity to respond to it or which has a significant impact on at least two Union entities; ~~too extensive for requiring more resources than are available at the affected Union institution, body or agency and entity and at CERT-EU to handle on their own;~~**

(9) 'incident handling' means incident handling **~~within the meaning of~~ as defined in** Article 4(6) of Directive [proposal NIS 2];

(10) 'cyber threat' means cyber threat **~~within the meaning of~~ as defined in** Article 2(8) of Regulation (EU) 2019/881;

(11) ~~**'significant cyber threat' means a cyber threat within the meaning of Article 4(7a) of Directive [proposal NIS 2] with the intention, opportunity and capability to cause a significant incident;**~~

(12) 'vulnerability' means vulnerability within the meaning of Article 4(8) of Directive [proposal NIS 2];

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

(14) '~~**cybersecurity**~~ risk' means **a risk within the meaning of Article 4(7b) of Directive [proposal NIS 2].** ~~**any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems;**~~

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

Article 3a

Processing of personal data

1) The processing of personal data under this Regulation by CERT-EU, the IICB or Union entities under this Regulation shall be carried out in compliance with ~~subject to~~ Regulation (EU) 2018/1725.

2) CERT-EU, the IICB and Union entities shall process and exchange personal data to the extent necessary and for the sole purpose of fulfilling their respective obligations under this Regulation. ~~Where pursuant to this Regulation, personal data is transmitted to recipients established in the Union other than Union institutions and bodies, this shall be done in accordance with the requirements laid down in Article 9 of Regulation (EU) 2018/1725.~~

Chapter II
MEASURES FOR A HIGH COMMON LEVEL OF CYBERSECURITY

Article 4

Risk management, governance and control framework

1. Each Union **~~institution, body and agency~~ entity** 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~~ The framework** shall be overseen by the entity's highest level of management to ensure an effective and prudent management of all cybersecurity risks. The framework shall be in place by …. at the latest [15 months after the entry into force of this Regulation].

2. The framework shall cover the entirety of the **unclassified** IT environment of the concerned **Union ~~institution, body or agency~~ entity**, including any on-premise IT environment, **operational technology network,** 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 **be based on ~~take account of~~ an all-hazard approach and on a maturity assessment in accordance with Article 6 covering all the relevant technical, operational and organisational risks that could impact the cybersecurity of the concerned Union entity ~~shall be considered.~~ ~~business continuity and crisis management and it shall consider risks posed to the security of network and information systems used by this entity for its operation, supply chain security as well as the management of human risks that could impact the cybersecurity of the concerned Union institution, body or agency.~~**

2a. **The framework shall lay down cybersecurity policies, including objectives and priorities for the security of network and information systems, and policies and procedures to assess the effectiveness of implemented cybersecurity risk management measures and define staff members' roles and responsibilities**.

2b. The framework shall be reviewed on a regular basis, and at least every [three years] in light of the changing risks, the assets and the maturity of the Union ~~institution, body or agency~~ entity.

3. The highest level of management of each Union **~~institution, body and agency~~ entity** shall **oversee ~~provide oversight over~~** the compliance of **~~their~~ its** organisation with the obligations related to cybersecurity risk management, governance, and control, without prejudice to the formal responsibilities of other levels of management for compliance and risk management in their respective areas of responsibility.

3aa. **Where appropriate and without prejudice to its responsibility for the implementation of this Regulation, the highest level of management of each Union entity may delegate to other senior officials within the entity concerned specific obligation under this Regulation. ~~Some tasks obligations of the highest level of management stemming from this Regulation may be, where appropriate, delegated to other senior officials of the Union entity.~~**

3a. The highest level of management of each Union entity shall ensure that the Union entities approve the cybersecurity risk management measures, in accordance ~~to~~ with their risk analysis, so that the framework is implemented in accordance with this Regulation. ~~The highest level of management of each Union entity shall oversee its implementation and~~ Regardless of possible delegation of its specific obligation ~~in accordance~~ pursuant to paragraph 3, ~~can~~ the highest level of management may be held liable for the non-compliance by the entities with the obligations under this ~~Article~~ Regulation.

~~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.~~

5. Each Union ~~institution, body and agency~~ **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.

The Local Cybersecurity Officer shall ~~be responsible for~~ facilitate the implementation of this Regulation and directly ~~inform~~ report to the highest level of management on a regular basis on the state of the implementation.

Without prejudice to the Local Cybersecurity Officer being a single point of contact in each Union entity, a Union entity may delegate ~~the~~ ~~competences~~ certain tasks of Local Cybersecurity Officer with respect to the implementation of this Regulation ~~may be delegated~~ to CERT-EU on ~~a~~ the basis of a service level agreement concluded between ~~the~~ that ~~concerned~~ Union ~~institution, body or agency~~ entity and CERT-EU. The IICB shall decide whether the provision of this service shall be part of the baseline services of CERT-EU ~~or service level agreement with CERT-EU~~, taking into account the human and financial resources of the concerned Union ~~institution, body or agency~~ entity. Appointed Local Cybersecurity Officers and any subsequent change thereto shall be notified by each Union ~~institution, body and agency~~ entity to the CERT-EU without undue delay. CERT-EU shall keep the regularly updated list of appointed Local Cybersecurity Officers.

5a. The senior officials within the meaning of Article 29(2) of the Staff Regulations[7] or other officials at equivalent level, of each Union ~~institution, body and agency~~ entity 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.~~

[7] Regulation No 259/68 of 29 February 1968 laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Communities, OJ L 56 of 4 March 1968.

6. Each Union ~~**institution, body and agency**~~ **entity** shall have effective mechanisms in place to ensure that an adequate percentage of the IT budget is spent on cybersecurity. **This percentage may be defined according to the framework referred to in paragraph 1.**

Article 5

Cybersecurity risk management measures ~~baseline~~

1. ~~**The**~~ **Each Union entity shall, under the oversight ~~authority~~ of ~~the~~ its** 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.**~~ **ensure that appropriate and proportionate technical, operational and organisational measures to manage the risks identified under the framework referred to in Article 4(1), and to prevent or minimise the impact of incidents, are taken. Having regard to the state of the art and, where applicable, relevant European and international standards, as well as the cost of implementation, those measures shall ensure a level of security of network and information systems appropriate to the ~~risk presented~~ risks posed. When assessing the proportionality of those measures, due account shall be taken of the degree of the entity's exposure to risks, its size, the likelihood of occurrence of incidents and their severity, including their societal and economic impact.**

2. Union ~~institutions, bodies and agencies~~ entities shall address at least the following specific domains in the implementation of the cybersecurity risk management measures within their cybersecurity plans, in line with the guidance documents and recommendations from the IICB:

(a) cybersecurity policy, ~~including~~ in terms of specification of the tools and measures needed to reach the objectives and priorities ~~for security of network and information systems, in particular regarding the use of cloud computing services within the meaning of~~ referred to in Article 4 ~~(19) of Directive [proposal NIS 2] and technical arrangements to enable teleworking;~~ and in Article 5 (3);

(b) risk analysis and information system security policies;

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

(d) asset management, including IT asset inventory and IT network cartography;

(e) human resources security and access control;

(f) operations security;

(g) communications security;

(h) system acquisition, development and maintenance, including vulnerability handling and disclosure;

(i) supply chain security including security related aspects concerning the relationships between each Union ~~institution, body and agency and its direct suppliers or service provider;~~ entity and its direct suppliers or service provider. Union entities shall take into account the vulnerabilities specific to each direct supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures;

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

(k) business continuity management, such as back-up management and disaster recovery, and crisis management; and

(l) promoting and developing cybersecurity education, skills, awareness-raising, exercise and training programmes.

3. Union ~~institutions, bodies and agencies~~ entities shall address at least the following specific cybersecurity risk management measures in the implementation of the cybersecurity risk management measures within their cybersecurity plans, in line with the guidance documents and recommendations from the IICB:

aa) objectives and priorities regarding the use of cloud computing services within the meaning of Article 4 (19) of Directive [proposal NIS 2] and technical arrangements to enable teleworking;

a) concrete steps for moving towards Zero Trust Architecture, which is to be understood as ~~(meaning~~ a security model, 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 establishment of software supply chain security through criteria for secure software development and evaluation;

d) 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 IT service providers about incidents, vulnerabilities and cyber threats with CERT-EU;

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

e) the use of cryptography and encryption, and in particular end-to-end encryption;

f) secured communication systems within the organisation, where appropriate.

~~**4. The senior management officials, as referred to in paragraph 2, within the meaning of Article 29(2) of the Staff Regulations[8] or other officials at adequate level, of each Union institution, body and agency entity 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.**~~

Article 6

Maturity assessments

1. Each Union ~~**institution, body and agency**~~ **entity** 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.

8 Regulation No 259/68 of 29 February 1968 laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Communities, OJ L 56 of 4 March 1968.

2. **The IICB, upon the recommendation of CERT-EU and after consulting the European Union Agency for Cybersecurity (ENISA), shall adopt methodological guidelines on conducting maturity assessments.**

3. **Upon completion of the maturity assessments, the Union ~~institutions, bodies and agencies~~ entities shall submit ~~these~~ it to the IICB. The first maturity assessment shall be carried out [12 months after the entry into force of this Regulation] at the latest.**

Article 7

Cybersecurity plans

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~~ entity** shall approve a cybersecurity plan **without undue delay** after the establishment of the **~~risk management, governance and control~~** framework, **~~and~~ adoption of** the **cybersecurity risk management measures ~~cybersecurity baseline~~ and carrying out of the maturity assessment ~~without undue delay~~ and no later than 21 months after the entry into force of this Regulation**. The **cybersecurity** plan shall aim at increasing the overall cybersecurity of the **~~concerned~~ Union** entity **concerned** and shall thereby contribute to the **~~achievement or~~** enhancement of a high common level of cybersecurity among all Union **~~institutions, bodies and agencies~~ entities. ~~To support the entity's mission on the basis of its institutional autonomy, the~~ The cybersecurity** plan shall at least include the **cybersecurity risk management measures ~~according~~ pursuant to Article 5 ~~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 **cybersecurity** plan shall be revised at least every **two ~~three~~** years, **or** following **every revision of** the maturity assessments carried out pursuant to Article 6 **or every revision of the framework ~~in accordance~~ pursuant to Article 4.**

2. ~~**The cybersecurity plan shall include staff members' roles and responsibilities for its implementation.**~~

3. The cybersecurity plan shall **take into account** ~~**consider**~~ any applicable guidance documents and recommendations issued **in accordance with Article 13** ~~**by CERT-EU**~~.

4. **Upon completion of the cybersecurity plans, the Union** ~~**institutions, bodies and agencies**~~ **entities shall** ~~**notify the IICB of the completion and**~~ **submit** ~~**them**~~ **it to the IICB**.

Article 7a

Peer Review

1. The IICB shall establish, at the latest by ... [24 months following the entry into force of this Regulation], using the methodology for peer reviews and methodology for self-assessment in accordance with Article 16 of Directive [proposal NIS 2] adapted where necessary to the needs of the Union ~~**institutions, bodies and agencies**~~ **entities, the methodology and organisational aspects of a peer review with a view to learning from shared experiences, strengthening mutual trust, achieving a high common level of cybersecurity, as well as enhancing the Union** ~~**institutions, bodies and agencies**~~ **entities cybersecurity capabilities and policies necessary to implement this Regulation. Participation in the peer reviews is voluntary. Representatives from Member States may participate** ~~**as observers**~~ **in the peer review as observers. The peer reviews shall be conducted by cybersecurity experts assigned by at least two Union** ~~**institutions, bodies and agencies**~~ **entities, different from the Union** ~~**institutions, bodies and agencies**~~ **entities being reviewed and shall cover at least one of the following:**

(i) the level of implementation of the cybersecurity risk management ~~**requirements**~~ **measures and reporting obligations referred to in Articles 5 and 20;**

(ii) the level of capabilities, including the available financial, technical and human resources~~, and the effectiveness of the exercise of the tasks of the national competent authorities;~~

~~(iii) the level of implementation of mutual assistance referred to in Article 22;~~

(iv) the level of implementation of the information-sharing framework, referred to in Article 19;

(v) specific issues of cross-sector nature.

2. Union ~~institutions, bodies and agencies~~ entities may identify specific issues mentioned in paragraph 1, point (v) to be reviewed. The scope of the review, including identified issues, shall be communicated to the participating Union ~~institutions, bodies and agencies~~ entities prior to the commencement of the peer review.

3. Prior to the commencement of the peer review, Union ~~institutions, bodies and agencies~~ entities may carry out a self-assessment of the reviewed aspects and provide that self-assessment to the designated experts. ~~The methodology for the self-assessment shall be defined by the Cooperation Group, with the support of the Commission and ENISA.~~

4. Peer reviews shall entail physical or virtual on-site visits and off-site exchanges. In view of the principle of good cooperation, the Union ~~institutions, bodies and agencies~~ entities subject to the peer review shall provide the designated experts with the information necessary for the assessment, without prejudice to national or Union laws concerning protection of confidential or classified information. ~~or to safeguard essential State functions, such as national security. The Cooperation Group, in cooperation with the Commission and ENISA, shall develop appropriate codes of conduct underpinning the working methods of designated experts.~~ Any information obtained through the peer review process shall be used solely for that purpose. The experts participating in the peer review shall not disclose any sensitive or confidential information obtained in the course of that review to any third parties.

5. Once subject to a peer review, the same aspects reviewed in the Union ~~institutions, bodies and agencies~~ entities, shall not be subject to further review in that Union ~~institutions, bodies and agencies~~ entities for the two years following the conclusion of the peer review, unless otherwise requested by the Union ~~institutions, bodies and agencies~~ entities or agreed upon after a proposal by the ~~Cooperation Group~~ IICB.

6. Union ~~institutions, bodies and agencies~~ entities shall ensure that any risk of conflict of interests concerning the designated experts are revealed to the other Union ~~institutions, bodies and agencies~~ entities and the ~~Cooperation Group, the Commission and ENISA~~ IICB, before the commencement of the peer review. The Union ~~institutions, bodies and agencies~~ entities subject to the peer review may object to the designation of particular experts on duly justified grounds communicated to the designating the Union ~~institutions, bodies and agencies~~ entities

7. Experts participating in peer reviews shall draft reports on the findings and conclusions of the reviews. Union ~~institutions, bodies and agencies~~ entities shall be allowed to provide comments on their respective draft reports, which shall be attached to the reports. The reports shall include recommendations to enable improvement on the aspects covered by the peer review. The reports shall be presented to the IICB and the CSIRTs network when relevant. Union ~~institutions, bodies and agencies~~ entities under review may decide to make its report, or a redacted version of its report, publicly available.

Article 8

Implementation

~~1. Upon completion of maturity assessments, the Union institutions, bodies and agencies shall submit these to the Interinstitutional Cybersecurity Board. Upon completion of security plans, the Union institutions, bodies and agencies shall notify the Interinstitutional Cybersecurity Board of the completion. Upon request of the Board, 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.

3. **Upon request of the IICB, the Union ~~institutions, bodies and agencies~~ entities shall report on specific aspects of this Chapter.**

Chapter III
INTERINSTITUTIONAL CYBERSECURITY BOARD

Article 9

Interinstitutional Cybersecurity Board

1. An Interinstitutional Cybersecurity Board (IICB) is established.

2. The IICB shall be responsible for:

   (a) monitoring the implementation of this Regulation by the **Union ~~institutions, bodies and agencies~~ entities**;

   (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) one representative designated by each of the following:

(i) the European Parliament;

(ii) the European Council

(iii) the Council of the European Union;

(iv) the European Commission;

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

(vi) the European Central Bank;

(vii) the European Court of Auditors;

(viii) the European External Action Service;

(ix) the European Economic and Social Committee;

(x) the European Committee of the Regions;

(xi) the European Investment Bank;

(xii) the European Union Agency for Cybersecurity; and

[(xiii) the Presidency of the Council of the European Union]

b) three representatives ~~**nominated**~~ **designated** 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:**~~

~~**(a) the European Parliament;**~~

~~**(b) the Council of the European Union;**~~

~~(c) the European Commission;~~

~~(d) the Court of Justice of the European Union;~~

~~(e) the European Central Bank;~~

~~(f) the European Court of Auditors;~~

~~(g) the European External Action Service;~~

~~(h) the European Economic and Social Committee;~~

~~(i) the European Committee of the Regions;~~

~~(j) the European Investment Bank;~~

~~(k) the European Union Agency for Cybersecurity;~~

~~(l) the current Presidency of the Council of the European Union.~~

Members may be assisted by an alternate. Other representatives of the **entities** ~~**organisations**~~ listed above or of other **Union** ~~**institutions, bodies and agencies**~~ **entities** may be invited by the chair to attend IICB meetings without voting power.

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 of the IICB for the same duration.

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

9. The Head of CERT-EU**, the chair of the NIS Cooperation Group**, **the chair of EU-CyCLONe and the chair of the CSIRTs Network,** or their ~~**his or her**~~ alternates, ~~**shall**~~ **may** participate in IICB meetings except where otherwise decided by the IICB**, as observers**.

10. The secretariat of the IICB shall be provided by the **ENISA** ~~**Commission**~~ **and shall be accountable to the IICB chair**.

11. The representatives nominated by the EUAN upon a proposal of the ICT Advisory Committee shall relay the IICB's decisions to the **members of the EUAN** ~~**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.

~~12. **The IICB may act by a simplified written procedure initiated by the chair under which the relevant decision shall be deemed approved within the timeframe set by the chair, except where a member objects**.~~

13. The IICB may nominate an Executive Committee to assist it in its work, and delegate some of its tasks and powers to it**, namely those in Article 10 letters (c), (e), and (k)**. 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.

14. **The IICB shall submit a report to the Council every 24 months detailing the progress made with the implementation of this Regulation and specifying in particular the extent of cooperation of CERT-EU with its national counterparts in each of the Member States. This report shall constitute an input to the biennial Report on the state of cybersecurity in the Union over the same time period in accordance to Article 15 of Directive [proposal NIS 2].**

Article 10

Tasks of the IICB

When exercising its responsibilities, the IICB shall in particular:

(a) ~~**review any reports requested from CERT-EU on the state**~~ **effectively monitor and supervise the application** ~~**of the provisions**~~ of this Regulation ~~**by**~~ **and support** the Union ~~**institutions, bodies and agencies**~~ **entities to strengthen their cybersecurity**; **to this end, the IICB may request ad-hoc reports from CERT-EU and Union** ~~**institutions, bodies and agencies**~~ **entities;**

(**aa**) **following a strategic discussion, adopt a multiannual strategy on raising the level of cybersecurity in the Union** ~~**institutions, bodies and agencies**~~ **entities and asses it on regular basis and at least every five years and where necessary, amend it;**

(b) approve, on the basis of a proposal **submitted by** ~~**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 **and any subsequent updates thereof**;

(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 key performance indicators 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;

(i) establish ~~as many~~ technical advisory groups ~~as necessary~~ to assist the IICB's work, approve their terms of reference and designate their respective chairs;

(j) **adopt guidance documents and recommendations on the basis of a proposal from CERT-EU in accordance with Article 13 and instruct CERT-EU to issue, withdraw or modify a proposal for guidance documents or recommendations, or a call for action;**

(k) receive and assess documents and reports submitted by the Union ~~institutions, bodies and agencies~~ entities under this Regulation;

(l) support the establishment of an informal group gathering the Local Cybersecurity Officers of all the entities and thereby facilitate the exchange of best practices and information in relation to the implementation of this Regulation;

(m) develop a cyber crisis management plan to support the coordinated management of major incidents at operational level affecting Union entities and to contribute to the regular exchange of relevant information.

Article 11

Compliance

1. The IICB shall**, in accordance with ~~the~~ Articles 9(2) and 10, effectively** monitor the implementation of this Regulation and of adopted guidance documents, recommendations and calls for action by the Union **~~institutions, bodies and agencies~~ entities**. **To this end, the IICB may request information or documentation necessary to assess ~~the implementation~~ the proper application of the provisions of the Regulation by the Union ~~institutions, bodies and agencies~~ entities. For the purpose of adopting compliance measures under this Article the concerned Union entity shall not have voting rights. ~~The IICB's decisions whether to issue compliance measures mentioned in paragraph 2 and 4 of this Article shall be taken by two-thirds majority of its members the concerned entity shall not have voting rights.~~**

2. Where the IICB finds that Union **entities ~~institutions, bodies or agencies~~** 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 **~~institution, body and agency~~ entity, and after having given the opportunity to the entity concerned to present its view**:

(a) issue a warning **to address identified shortcomings within a specified timeframe, including recommendations to amend cybersecurity documents adopted by the Union ~~institutions, bodies and agencies~~ entities based on this Regulation. ~~The entity concerned shall provide feedback to the IICB as to what action it has taken and will take to address the issues mentioned in the recommendation~~;** where necessary in view of a compelling cybersecurity risk, the audience of the warning shall be restricted appropriately;

(aa) issue ~~reprimands~~ a reasoned notification to a Union entity, in case that shortcomings identified in the previously issued warning were not sufficiently addressed in a specified timeframe, and formally notify that opinion ~~those~~ to the Council, the European Parliament and the Commission.

(b) ask for an audit of the Union entity to be carried out, in particular: ~~recommend a relevant audit service to carry out an audit. In duly justified cases, order request the audit of the Union institutions, bodies and agencies entities by a [mutually agreed] third party audit service;~~

i. recommend that an audit of a Union entity is carried out;

ii. request that an audit is carried out, where the Union entity concerned does not have established an internal audit function pursuant to Article 117 of the Regulation (EU) 2018/1046 of the European Parliament and of the Council, the IICB may suggest a relevant audit services;

iii. in duly justified cases, request that an audit is performed by a [*mutually agreed*] third party audit services.

(c) request the Union entity to bring the management, governance and control of cybersecurity risks into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;

(d) issue an advisory to all Member States and Union entities recommending temporary suspension of data flows to ~~a~~ the Union entity.

3. Where the IICB has adopted measures under ~~exercises the powers provided for in~~ paragraph 2 points (a) - (d), the Union entity concerned shall provide a detailed account of the measures and actions taken to address the alleged shortcomings identified by the IICB. The Union entity shall submit this account within a reasonable period to be agreed with the IICB. ~~inform the IICB of its feedback within a reasonable period to be specified by the IICB taking into account the circumstances of each case. The reply shall also include a description of the measures taken, if any, in response to the remarks of the IICB.~~

4. ~~Deliberate and long term deviation of the provisions of this Regulation and failing to apply necessary action to remedy the deficiencies or comply with the requirements of the IICB and/or provisions of this Regulation may be a reason for opening disciplinary proceedings against any member of the highest level of management discharging managerial responsibilities in regards to this Regulation in that entity by the respective appointing authority. This paragraph is without prejudice to the administrative investigation powers of the relevant Appointing Authority in accordance to the Staff Regulations.~~

Where the IICB considers that there is a continuous breach of the provisions of this Regulation by a Union entity resulting directly from actions or omissions of an official or other servant of the Union, including at the highest level of management, the IICB shall request the entity concerned to take the appropriate actions, including of disciplinary nature, in accordance, in particular, with the rules laid down in the Staff Regulations and the Conditions of employment of other servants of the European Union. For this purpose, the IICB shall transfer the necessary information to the entity concerned.

Chapter IV
CERT-EU

Article 12

CERT-EU mission and tasks

1. ~~**The mission of CERT-EU, the An autonomous interinstitutional computer emergency response team, named CERT-EU, [shall be established] Cybersecurity Centre for all Union institutions, bodies and agencies,**~~ **CERT-EU´s mission**~~**, as an autonomous interinstitutional computer emergency response team,**~~ **shall be to** contribute to the security of the unclassified IT environment of all Union ~~**institutions, bodies and agencies**~~ **entities** 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.

1a. CERT-EU shall collect, manage, analyse and share information with the Union entities ~~**constituents**~~ **on threats, vulnerabilities and incidents on unclassified ICT infrastructure. It shall coordinate responses to incidents at inter-institutional and Union entity** ~~**constituent**~~ **level, including by providing or coordinating the provision of specialised operational assistance.**

2. CERT-EU shall perform the following tasks for the Union ~~**institutions, bodies and agencies**~~ **entities**:

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

   (b) ~~**support them with**~~ **offer standard CERT services for all Union entities through** a package of cybersecurity services described in its service catalogue (‘baseline services’);

(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 the guidance documents, recommendations and calls for action;

(e) report **to the Union ~~institutions, bodies and agencies~~ entities** on ~~**the**~~ **relevant** cyber threats ~~**faced by the Union institutions, bodies and agencies**~~ and contribute to the EU cyber situational awareness **in close cooperation with ENISA. Such reports shall be shared with the IICB, as well as the CSIRTs Network and EU-INTCEN ~~CyCLONe and the NIS Cooperation Group~~.**

(f) act as the equivalent of the designated coordinator for the Union ~~institutions, bodies and agencies~~ entities, for the purpose of coordinated vulnerability disclosure to the European vulnerability registry as referred to in Article 6 of Directive [proposal NIS 2].

~~**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 institutions, bodies and agencies**~~

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

~~**(c) cyber threat intelligence, including situational awareness;**~~

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

4. **Within the framework of competences,** CERT-EU shall engage in structured cooperation with ~~**the European Union Agency for Cybersecurity**~~ **ENISA** 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.

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

   (a) services that support the cybersecurity of Union ~~**institutions, bodies and agencies**~~ **entities'** IT environment, other than those referred to in paragraph 2, on the basis of service level agreements and subject to available resources;

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

   (c) services that support the security of their IT environment to organisations other than the Union ~~**institutions, bodies and agencies**~~ **entities** that cooperate closely with Union ~~**institutions, bodies and agencies**~~ **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 may organise **or participate in** cybersecurity exercises or recommend participation in existing exercises, in close cooperation with ~~**the European Union Agency for Cybersecurity**~~ **ENISA** whenever applicable, to test the level of cybersecurity of the Union ~~**institutions, bodies and agencies**~~ **entities**.

7. CERT-EU may provide assistance to Union ~~institutions, bodies and agencies~~ **entities** regarding incidents in classified IT environments if it is explicitly requested to do so by the **Union entities** ~~constituent~~ **concerned in accordance with their respective procedures. In this case the provisions set out in Articles 19 to 21 of this Regulation shall not apply.**

8. CERT-EU shall inform Union entities about its incident handling procedures and processes.

9. CERT-EU may monitor Union entities' network traffic with the consent of the relevant Union entity ~~constituent~~**.**

10. CERT-EU may, if expressly requested by Union entities' policy departments, ~~contribute its~~ **provide technical advice or input on relevant policy matters.**

11. CERT-EU shall, in cooperation with the European Data Protection Supervisor, support the ~~concerned~~ **Union entities concerned** ~~in cooperation with the EDPS~~ **when addressing incidents resulting in personal data breaches.**

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 ~~institutions, bodies and agencies~~ **entities** are urged to take within a set timeframe**. Without undue delay after receiving the call for action the concerned Union entity shall provide an information to CERT-EU, how those measures were applied**;

   (b) proposals to the IICB for guidance documents addressed to all or a subset of the Union ~~institutions, bodies and agencies~~ **entities**;

   (c) proposals to the IICB for recommendations addressed to individual Union ~~institutions, bodies and agencies~~ **entities**.

2. Guidance documents and recommendations may include:

(a) modalities for or improvements to cybersecurity risk management and the cybersecurity **risk management measures ~~baseline~~**;

(b) modalities for maturity assessments and cybersecurity plans; and

(c) where appropriate, the use of common technology, architecture and associated best practices with the aim of achieving interoperability and common standards ~~**within the meaning of Article 4(10) of Directive [proposal NIS 2].**~~

~~**3. The IICB may adopt guidance documents or recommendations on proposal of CERT-EU.**~~

~~4.~~ ~~**The IICB may instruct CERT-EU to issue, withdraw or modify a proposal for guidance documents or recommendations, or a call for action.**~~

Article 14

Head of CERT-EU

1. The Commission, after having obtained the ~~unanimous~~ approval by two-thirds of the members of the IICB, 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 this post.

2. The Head of CERT-EU shall be responsible for the proper functioning ~~smooth running~~ of CERT-EU, acting within its remit under the direction of the IICB. He or she shall be responsible for implementing the strategic direction, guidance, objectives and priorities set by the IICB, and for the ~~sound~~ management of CERT-EU, including of its financial and human resources. He or she shall report regularly to the IICB Chair.

3. The Head of CERT-EU shall assist the responsible authorising officer by delegation in drafting the annual activity report containing financial and management information, including the results of controls, drawn up in accordance with Article 66(9) of the Financial Regulation, and shall report regularly to him or her on the implementation of measures in respect of which powers have been sub-delegated to him.

4. The Head of CERT-EU shall draw up annually a financial planning of administrative revenue and expenditure for its activities, the annual work programme proposal, ~~the~~ CERT-EU ´s service catalogue proposal and ~~its~~ the revision thereof, the proposal of modalities for service level agreements and the proposal of key performance indicators for CERT-EU to be approved by the IICB in accordance with Article 10.

When revising the list of services in ~~the~~ CERT-EU's service catalogue, the Head of CERT-EU shall take into account the resources allocated to ~~him or her~~ CERT-EU.

5. The Head of CERT-EU shall ~~**regularly**~~ ~~**annually**~~ submit **annual** 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(~~**1a**~~**a**).

Article 15

Financial and staffing matters

~~1. **The Commission, after having obtained the unanimous approval of the IICB, 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 this post.**~~

1a. **While established as an autonomous interinstitutional service provider for all Union entities, CERT-EU shall be 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 shall be evaluated on a regular basis, at the latest before the end of any future long-term budget framework decided on by Article 312 TFEU to allow for appropriate action to be taken.**

2. For the application of administrative and financial procedures, the Head of CERT-EU shall act under the authority of the Commission.

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~~ **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 ~~institutions, bodies and agencies~~ **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].

[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).

5. The costs of the tasks defined in Article 12(5) shall be recovered from the Union ~~institutions, bodies and agencies~~ **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 **without undue delay** cooperate and exchange information with national counterparts in the Member States, **notably ~~including~~ ~~CERTs,~~ ~~national competent authorities~~ ~~National Cybersecurity Centres~~,** CSIRTs **referred to in Article 9 of Directive [proposal NIS 2]**, **national competent authorities** 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~~ **entities**, including through the CSIRTs network referred to in Article 13 of Directive [proposal NIS 2].

1a. **CERT-EU shall, without delay, notify the national counterpart in a Member State, in case of activities related to significant incidents occurring within the territory of the national counterpart of CERT-EU.**

2. CERT-EU **shall without undue delay ~~may~~** exchange incident-specific information with national counterparts in the Member States to facilitate detection of similar cyber threats or incidents **or to contribute to the analysis of an incident** without **needing** the consent of the affected **Union entity ~~constituent~~**. CERT-EU **shall not ~~may only~~** exchange incident-specific information which reveals the identity of the target of the cybersecurity incident **unless ~~with the consent of the affected constituent.~~**

(a) there is consent of the affected Union entity ~~constituent~~;

(b) the affected Union entity ~~constituent~~ already published that it was affected;

(c) there is no consent of the affected Union entity ~~constituent~~, but the publication of the identity of the affected Union entity ~~constituent~~ would increase the probability that incidents elsewhere will be avoided or mitigated. Such decisions require the approval of the Head of CERT-EU. The affected Union entity ~~constituent~~ shall be informed before the publication.

~~**[3. The cooperation and exchange of information under this Article shall be without prejudice to Article 18 paragraph 5.]**~~

Article 17

Cooperation of CERT-EU with ~~non-Member State~~ other counterparts

1. CERT-EU may cooperate with ~~**non-Member State**~~ counterparts **in the European Union other than those mentioned in Article 16,** 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 **on a case-by-case basis. CERT-EU shall inform the national CSIRT of the Member State, in which the counterpart is located, when CERT-EU cooperates with such counterparts.**

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 **on a case-by-case basis.**

3. CERT-EU may, **provided a non-disclosure arrangement or contract is in place with the relevant partner,** with the consent of the **Union entity ~~constituent~~** affected by an incident, provide information related to **specific** incident to partners **referred to in paragraphs 1 and 2 solely for the purpose of contributing ~~that can contribute~~** to its analysis. **Such non-disclosure agreements or contracts shall be legally verified in accordance with the relevant internal Commission procedures. Non-disclosure agreements or contracts shall not require prior approval by the IICB, but ~~its~~ the chair of the IICB shall be informed.**

4. **CERT-EU may exceptionally enter into service level arrangements with entities other than the Union entities ~~constituents~~ with the prior approval of the IICB.**

Chapter V
COOPERATION AND REPORTING OBLIGATIONS

Article 18

Information handling

1. CERT-EU and Union **~~institutions, bodies and agencies~~ 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[10] 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~~ entities, and where relevant the Member States,** whenever a request concerns their documents.

[10] 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).

~~**3. The processing of personal data carried out under this Regulation shall be subject to Regulation (EU) 2018/1725 of the European Parliament and of the Council.**~~

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

~~**[4a. CERT-EU shall not initiate activities or knowingly intervene in any matters that fall within the competence of national security. and intelligence]**~~

~~**[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.]**~~

Article 19

~~Sharing~~ Cybersecurity information sharing obligations

-1. Union entities may voluntarily provide ~~to the~~ 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.

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

2. The Union ~~**institutions, bodies and agencies**~~ **entities**, 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.

3. CERT-EU may **only** exchange incident-specific information **with the Union** ~~**institutions, bodies and agencies**~~ **entities** which reveals the identity of the Union ~~**institution, body and agency**~~ **entity** affected by the incident with the consent of that entity. **Where consent is withheld, the entity concerned shall provide duly justified reasons to CERT-EU.** ~~**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.**~~

~~[~~4. The sharing obligations shall not extend to EU Classified Information (EUCI) and to information **related to national security** that a Union **entity** ~~**institution, body or agency**~~ has received from **other Member State competent authorities unless that Member State competent authority explicitly allows this information to be shared with CERT-EU.** ~~**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 20

~~***Notification***~~ ***Reporting obligations***

-1. An incident shall be considered to be significant if:

(a) it 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;

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

1. All Union ~~institutions, bodies and agencies~~ **entities** shall **submit** ~~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.~~

~~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~~.

(a) without undue delay and in any event within 24 hours after having become aware of the significant incident, an early warning, which, where applicable, shall indicate whether the significant incident is presumably caused by unlawful or malicious action and has ~~any~~ or could have a cross-border impact;

(b) without undue delay and in any event within 72 hours after having become aware of the significant incident, an incident notification, which, where applicable, shall update the information referred to in subparagraph (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;

(d) a final report not later than one month after the submission of the significant incident notification under point (b), including at least the following:

(i) a detailed description of the significant incident, its severity and impact;

(ii) the type of threat or root cause that likely triggered the significant incident;

(iii) applied and ongoing mitigation measures.

(iv) where applicable, the cross-border impact of the significant incident;

(e) in cases of ongoing significant incidents at the time of the submission of the final report referred to in point (d), a progress report at that time and a final report within one month after the incident has been handled.

~~**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:**~~

~~**(a) relevant indicators of compromise;**~~

~~**(b) relevant detection mechanisms;**~~

~~**(c) potential impact;**~~

~~**(d) relevant mitigating measures.**~~

2a. All Union ~~institutions, bodies and agencies~~ entities shall share the information within the timeline defined in paragraph 1 with the CSIRT or national competent authority of the Member State where it is located.

3. CERT-EU shall submit to **~~ENISA,~~ the IICB, the EU INTCEN and the CSIRTs Network every three months ~~on a monthly basis~~** a summary report including anonymised and aggregated data on **~~significant~~** cyber threats, **~~significant~~** vulnerabilities **in accordance with Article 19, Union entities' replies to calls for action in accordance with Article 13 paragraph 1 letter (a)** and significant incidents notified in accordance with paragraph 1. **Th~~at~~is report shall constitute an input to the biennial report on the state of cybersecurity in the Union ~~in accordance to~~ under Article 15 of Directive [proposal NIS 2].**

4. The IICB **shall, ~~may~~ ~~issue~~ by [6 ~~12~~] months after the date of entry into force of this Regulation, issue** guidance documents or recommendations **further specifying ~~concerning~~** the modalities, **format** and content of the **reporting ~~notification~~**. **The guidance documents or recommendations shall duly take into account the provisions being implemented by any implementing acts according to paragraph 11 of Article 20 of Directive [proposal NIS 2]** CERT-EU shall disseminate the appropriate technical details to enable proactive detection, incident response or mitigating measures by Union **~~institutions, bodies and agencies~~ entities**.

~~[~~5. The **reporting ~~notification~~** obligations shall not extend to EUCI and to information **related to national security** that a Union **~~institution, body and agency~~ entity** has received from **other Member State competent authorities unless that Member State competent authority explicitly allows this information to be shared with CERT-EU. ~~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 ~~on significant incidents~~

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 and incidents among:

   (a) Union **~~institutions, bodies and agencies~~ entities**;

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

2. CERT-EU**,** ~~and~~ **where relevant in close cooperation with ENISA in accordance with Article 7 paragraph 7 (d) of the Cybersecurity Act[11],** shall facilitate coordination among Union ~~institutions, bodies and agencies~~ **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 close cooperation with ENISA** shall support Union ~~institutions, bodies and agencies~~ **entities** regarding situational awareness of cyber threats, vulnerabilities and incidents.

4. The IICB shall**,** ~~issue~~ **by [12] months after the date of entry into force of this Regulation, issue** guidance **documents or recommendations** 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.

Article 22

Major incidents ~~attacks~~

-1. In order to support the coordinated management of major incidents at operational level affecting Union entities and to contribute to the regular exchange of relevant information among Union entities and with Member States, the IICB shall develop a cyber crisis management plan based on activities detailed in Article 21(2), in close cooperation with CERT-EU and ENISA, and shall include, at least, the following elements:

[11] 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)

(a) coordination and information flow modalities among Union entities for the management of major incidents at operational level;

(b) common standard operating procedures (SOPs);

(c) a common taxonomy of crisis functions and crisis triggering points;

(d) regular exercises;

(e) secure communication channels to be used;

(f) a point of contact for the EU-CyCLONe, which will share relevant information with the EU-CyCLONe as inputs to shared situational awareness.

1. CERT-EU shall coordinate among Union **~~institutions, bodies and agencies~~ entities** responses to major **incidents ~~attacks~~**. It shall maintain an inventory of technical expertise that would be needed for incident response in the event of **major incidents ~~such attacks~~**.

2. The Union **~~institutions, bodies and agencies~~ 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. **Following a specific request from a Member State in which the affected Union entity is located and with ~~With~~** the approval of the **affected ~~concerned~~** Union **~~institutions, bodies and agencies~~ entities**, CERT-EU may also call on experts from the list referred to in paragraph 2 for contributing to the response to a major **incident ~~attack~~ in ~~a~~ that Union entity ~~Member State, in line with the Joint Cyber Unit's operating procedures~~.**

Chapter VI
FINAL PROVISIONS

Article 23

Initial budgetary reallocation

The Commission shall propose the reallocation of staff and financial resources from relevant Union ~~**institutions, bodies and agencies**~~ **entities** 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 Regulation.

Article 24

Review

1. The IICB, with the assistance of CERT-EU, shall periodically report to the Commission on the implementation of this Regulation. The IICB may also make recommendations to the Commission to **review** ~~**propose amendments to**~~ this Regulation.

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

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 **later** ~~**sooner**~~ than five years after the date of entry into force.

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 Brussels,

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

~~**ANNEX I**~~

~~**The following domains shall be addressed in the cybersecurity baseline:**~~

~~**(1) cybersecurity policy, including objectives and priorities for security of network and information systems, in particular regarding the use of cloud computing services (within the meaning of Article 4(19) of Directive [proposal NIS 2]) and technical arrangements to enable teleworking;**~~

~~**(2) organisation of cybersecurity, including definition of roles and responsibilities;**~~

~~**(3) asset management, including IT asset inventory and IT network cartography;**~~

~~**(4) access control;**~~

~~**(5) operations security;**~~

~~**(6) communications security;**~~

~~**(7) system acquisition, development and maintenance;**~~

~~**(8) supplier relationships;**~~

~~**(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;**~~

~~**(10) business continuity management and crisis management; and**~~

~~**(11) cybersecurity education, awareness-raising and training programmes.**~~

~~**ANNEX II**~~

~~**Union institutions, bodies and agencies shall address at least the following specific cybersecurity measures in the implementation of the cybersecurity baseline and in their cybersecurity plans, in line with the guidance documents and recommendations from the HCB:**~~

~~**(1) concrete steps for moving towards Zero Trust Architecture (meaning a security model, 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);**~~

~~**(2) the adoption of multifactor authentication as a norm across network and information systems;**~~

~~**(3) the establishment of software supply chain security through criteria for secure software development and evaluation;**~~

~~**(4) the enhancement of procurement rules to facilitate a high common level of cybersecurity through:**~~

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

~~**(b) the contractual obligation to report incidents, vulnerabilities and cyber threats as well as to have appropriate incidents response and monitoring in place.**~~