Council of the European Union

Brussels, 18 September 2023
(OR. en)

12999/23

Interinstitutional File: 2022/0085(COD)

CYBER 214
TELECOM 266
INST 338
CSC 442
CSCI 161
INF 205
FIN 927
BUDGET 26
DATAPROTECT 235
CODEC 1597

INFORMATION NOTE

From:	General Secretariat of the Council
To:	Delegations
No. prev. doc.:	12676/23
No. Cion 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 - Letter sent to the European Parliament

At its meeting on 15 September 2023, the Permanent Representatives Committee (Part 2)

a) confirmed the agreement on the compromise text of the above-mentioned draft Regulation, as it was reached between the negotiating parties on 26 June 2023 and as it is contained in 12676/23; and

b) authorised the Presidency to address the habitual offer letter to the European Parliament.

The letter as it was sent to the European Parliament is set out in the Annex.

This information is provided in accordance with point 1 h) of note 9493/20 on ‘Strengthening legislative transparency’.

Council of the European Union

SGS 23 / 003917

Brussels, 15/09/2023

Mr Cristian Silviu BUŞOI
Chair of the Committee on Industry, Research and Energy
European Parliament
Rue Wiertz 60
B-1047 BRUSSELS

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

Dear Mr BUŞOI,

Following the informal negotiations on this proposal between the representatives of the three institutions, today the Permanent Representatives Committee agreed with the final compromise text.

I am therefore now in a position to inform you that, should the European Parliament adopt its position at first reading, in accordance with Article 294(3) TFEU, in the exact form of the text set out in the Annex to this letter (subject to revision by the lawyer-linguists of the two institutions), the Council, in accordance with Article 294(4) TFEU, will approve the European Parliament's position and the act shall be adopted in the wording which corresponds to the position of the European Parliament.

On behalf of the Council, I also wish to thank you for your close cooperation which should enable us to reach agreement on this file at first reading.

Yours sincerely

Marcos ALONSO ALONSO
Chair of the
Permanent Representatives Committee

Copy:
- Mr Johannes HAHN, Commissioner
- Ms Henna VIRKKUNEN, European Parliament rapporteur

Rue de la Loi/Wetstraat 175 – 1048 Bruxelles/Brussel – Belgique/België
Tél./Tel. +32 (0)2 281 61 11

ANNEX

2022/0085 (COD)

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, ***the*** ubiquitous use of ***information and communication technology (ICT)***, high digitalisation, remote work and evolving technology and connectivity are nowadays core features of all activities of the Union administration entities, digital resilience is not yet sufficiently built in.

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

(3) The Union ***entities' ICT*** environments have interdependencies, integrated data flows and their users collaborate closely. This interconnection means that any disruption, even when initially confined to one Union ***entity***, can have cascading effects more broadly, potentially resulting in far-reaching and long-lasting negative impacts on the others. In addition, certain ***Union entities' ICT*** environments are connected with Member States' ***ICT*** environments, causing an incident in one Union entity to pose a risk to the cybersecurity of Member States' ***ICT*** environments and vice versa. ***Sharing incident-specific information may facilitate the detection of similar cyber threats or incidents affecting Member States***.

(4) The Union ***entities*** are attractive targets who face highly skilled and well-resourced threat actors as well as other threats. At the same time, the level and maturity of cyber resilience and the ability to detect and respond to malicious cyber activities varies significantly across those entities. It is thus necessary for the functioning of the European administration that the ***Union entities*** achieve a high common level of cybersecurity through ***implementation of*** cybersecurity***measures commensurate with identified*** risks, information exchange and collaboration.

(5) Directive ***(EU) 2022/2555 of the European Parliament and of the Council***[1] aims to further improve the cybersecurity resilience and incident response capacities of public and private entities, national competent authorities and bodies as well as the Union as a whole. It is therefore necessary that Union ***entities*** follow suit by ensuring rules that are consistent with Directive ***(EU) 2022/2555*** and mirror its level of ambition.

[1] ***Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80).***

(6) To reach a high common level of cybersecurity, it is necessary that each Union ***entity*** establishes ***a*** 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. ***That framework should lay down cybersecurity policies and priorities for the security of network and information systems encompassing the entirety of the unclassified ICT environment. The framework should be based on an all-hazard approach, which aims to protect network and information systems and the physical environment of those systems, from events such as theft, fire, flood, telecommunication or power failures, or unauthorised physical access and damage to, and interference with Union entity's information and information processing facilities, which could compromise the availability, authenticity, integrity or confidentiality of data stored, transmitted, processed or accessible via network and information systems.***

(6a) To manage the risks identified under the framework, each Union entity should ensure that appropriate and proportionate technical, operational and organisational measures are taken. These should address the domains and specific cybersecurity risk management measures set out in this Regulation to strengthen the cybersecurity of each Union entity.

(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.

(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 entities. The framework should be reviewed on a regular basis and at least every four years, while the cybersecurity plan should be revised at least every two years, or when necessary, following the maturity assessments or any substantial review of the framework.

(6e) A mechanism to ensure effective 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 involved Union entities. The Commission representative in the IICB should, subject to the conditions provided for in the cyber crisis management plan, be the point of contact to facilitate the IICB's sharing of relevant information in relation to major incidents with EU-CyCLONe, as a contribution to the shared situational awareness. That role of the Commission representative in the IICB as point of contact should be without prejudice to the Commission's separate and distinct role in EU-CyCLONe under Article 16(2) of Directive (EU) 2022/2555.

(7) The differences between Union ***entities*** require flexibility in the implementation since one size will not fit all. The measures for a high common level of cybersecurity should not include any obligations directly interfering with the exercise of the missions of Union ***entities*** or encroaching on their institutional autonomy. ***Therefore***, those ***entities*** should establish their own frameworks for cybersecurity risk management, governance and control, and adopt their own ***cybersecurity risk-management measures*** and cybersecurity plans. ***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 optimisation. Due account should also be taken that the measures do not negatively affect the Union entities' efficient information exchange and operations with other Union entities and national counterparts.***

(7a) In the interest of optimizing the use of resources, this Regulation should provide for the possibility for two or more Union entities to cooperate in carrying out the cybersecurity maturity assessments.

(8) In order to avoid imposing a disproportionate financial and administrative burden on Union ***entities***, the cybersecurity ***risk-management*** requirements should be proportionate to the risk presented by the network and information system concerned, taking into account the state of the art of such measures. Each Union ***entity*** should aim to allocate an adequate percentage of its ***ICT*** budget to improve its level of cybersecurity; in the longer term ***an indicative*** target in the order of ***at least*** 10% should be pursued. ***The maturity assessment should also assess whether the Union entity's cybersecurity spending is proportionate to the risks it faces. Without prejudice to the rules relating to the Union's annual budget under the Treaties, in its proposal for the first budget to be adopted after the entry into force of this Regulation the Commission should take into account the obligations arising from this Regulation when assessing the budgeting and staffing needs of the Union entities as resulting from their estimates of expenditures.***

(9) A high common level of cybersecurity requires cybersecurity to come under the oversight of the highest level of management of each Union ***entity***. ***The highest level of management*** should ***be responsible for the implementation of this Regulation, including establishment of the risk management, governance and control framework and cybersecurity plans, encompassing cybersecurity measures***. Addressing the cybersecurity culture, i.e. the daily practice of cybersecurity, is an integral part of a cybersecurity ***risk-management, governance and control framework and the corresponding cybersecurity risk-management measures*** in all Union ***entities***.

(10) Union ***entities*** should assess risks related to relationships with suppliers and service providers, including providers of data storage and processing services or managed security services, and take appropriate measures to address them. ***Cybersecurity*** measures should ▌ be further specified in guidance documents or recommendations issued by CERT-EU. When defining measures and guidelines, due account should be taken of ***the state of the art and, where applicable,*** relevant ***European and international standards, as well as relevant Union law*** and policies, including risk assessments and recommendations issued by theNIS Cooperation Group, such as the EU Coordinated risk assessment and EU Toolbox on 5G cybersecurity. In addition, ***considering the threat landscape and the importance of building up resilience for the Union entities*** certification of relevant ICT products, services and processes could be required, under specific ***Union*** cybersecurity certification schemes adopted pursuant to Article 49 of Regulation EU 2019/881.

(11) In May 2011, the Secretaries-General of the Union institutions and bodies decided to establish a pre-configuration team for a computer emergency response team for the Union's institutions, bodies and agencies (CERT-EU) supervised by an inter-institutional Steering Board. In July 2012, the Secretaries-General confirmed the practical arrangements and agreed to maintain CERT-EU as a permanent entity to continue to help improve the overall level of information technology security of the Union's institutions, bodies and agencies as an example of visible inter-institutional cooperation in cybersecurity. In September 2012, CERT-EU was established as a Taskforce of the European Commission with an interinstitutional mandate. In December 2017, the Union institutions and bodies concluded an interinstitutional arrangement on the organisation and operation of CERT-EU [2]. ***This Regulation*** should ***provide a comprehensive set of rules on the organisation, functioning and operation of CERT-EU. The provisions*** of this Regulation ***prevail over provisions of the interinstitutional arrangement on the organisation and operation of CERT-EU that was concluded in December 2017***.

[2] OJ C 12, 13.1.2018, p. 1–11.

(12) CERT-EU should be renamed from ‘computer emergency response team’ to ‘Cybersecurity ***Service***’ for the Union institutions, bodies ***, offices and agencies***, but it should keep the short name ‘CERT-EU’ because of name recognition.

(12a) This Regulation should be evaluated on a regular basis in light of future negotiations of long-term budget frameworks, allowing for further decisions to be made with respect to the functioning and institutional role of CERT-EU, including the possible establishment of CERT-EU as a Union office.

(13) Many cyberattacks are part of wider campaigns that target groups of Union ***entities*** or communities of interest that include Union ***entities***. To enable proactive detection, incident response or mitigating measures ***and recovery from significant incidents***, Union ***entities*** should notify CERT-EU of ▌ cyber threats, ▌ vulnerabilities***, near misses and*** 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 ***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 ***early warning*** to CERT-EU within 24 hours. Such information exchange should enable CERT-EU to disseminate the information to other Union ***entities***, as well as to appropriate counterparts, to help protect the Union ***ICT*** environments and the Union's counterparts' ***ICT*** environments against similar incidents▌ .

(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 hand, in-depth reporting that draws valuable lessons from individual incidents and improves over time the cyber resilience of individual Union entities and contributes to increasing their overall cybersecurity posture. In that regard, this Regulation should include the reporting of incidents that, based on an initial assessment carried out by the Union entity concerned, 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 natural or legal persons could play an important role in identifying whether the operational disruption is severe.

(13b) The security of network and information systems handling EU classified information (EUCI) is essential. Union entities handling EUCI are required to apply the comprehensive regulatory frameworks in place for protecting such information, including specific governance, policies and risk management procedures. It is necessary for network and information systems handling EUCI to be subject to more stringent security standards than unclassified network and information systems. Therefore, network and information systems handling EUCI are more resilient to cyber threats and incidents. Consequently, while recognising the need for a common framework in this regard, this Regulation should not apply to network and information systems handling EUCI. However, if explicitly requested to do so by a Union entity, CERT-EU should be able to provide assistance to that Union entity in relation to incidents in classified ICT environments.

(13c) As the infrastructure and networks of the relevant Union entity and the Member State where that Union entity is located are interconnected, it is crucial for that Member State to be informed without undue delay of a significant incident within that Union entity. For that purpose, the affected Union entity should inform CERT-EU's national counterpart, designated by the Member State in accordance with the Directive (EU) 2022/2555 of the occurrence of a significant incident, regarding which it is reporting to CERT-EU. CERT-EU should also notify this national counterpart when it becomes aware of a significant incident within the Member State.

(14) In addition to giving CERT-EU more tasks and an expanded role, an Interinstitutional Cybersecurity Board (IICB) should be established ***which, in order to*** facilitate a high common level of cybersecurity among Union ***entities, should have an exclusive role in*** monitoring the implementation of this Regulation by the Union ***entities and in*** supervising implementation of general priorities and objectives by CERT-EU and providing strategic direction to CERT-EU. The IICB should ***therefore*** ensure 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 political 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 establish 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 require specific expertise of its members, for instance the approval of the service catalogue and any subsequent updates to it, modalities for service level agreements, assessments of documents and reports submitted by the Union entities to the IICB according to this Regulation or tasks related to the preparation of decisions on compliance measures issued by the IICB and to monitoring of their implementation. The IICB should lay down the rules of procedures of the Executive Committee, including its tasks and powers.***

(*14a) The IICB aims to support entities in elevating their respective cybersecurity postures by implementing this Regulation. In order to support Union entities, the IICB should provide guidance to the head of CERT-EU, adopt a multiannual strategy on raising the level of cybersecurity in the Union entities, establish the methodology and aspects for voluntary peer reviews, and facilitate the establishment of an informal group of Local Cybersecurity Officers, supported by ENISA, with an aim to exchange best practices and information in relation to the implementation of this Regulation*.

(14b) In order to achieve a high level of cybersecurity in all the Union entities, the interests of the bodies and agencies of the Union that run their own ICT environment should be represented in the IICB by three representatives designated by the Union Agencies Network (EUAN). The security of personal data processing, and therefore also the cybersecurity thereof, is a cornerstone for data protection. In light of the synergies between data protection and cybersecurity, the EDPS should be represented in the IICB in their capacity as a Union entity subject to this Regulation, with specific expertise in the area of data protection including security of electronic communications networks. In light of the role assigned to CERT-EU under this Regulation, the Head of CERT-EU should be invited systematically by the chair of the IICB, except when the IICB discusses matters relating directly to the Head of CERT-EU. Considering the importance of innovation and competitiveness in cybersecurity, the European Cybersecurity Industrial, Technology and Research Competence Centre should be represented in the IICB. Similarly, in view of the role of ENISA as a centre of expertise in cybersecurity, and the support it provides, ENISA should also be represented in the IICB. Similarly, in view of the importance of cybersecurity of Union space infrastructure and services, the European Union Agency for the Space Programme should be represented in the IICB.

(15) CERT-EU should support the implementation of measures for a high common level of cybersecurity through proposals for guidance documents and recommendations to the IICB or by issuing calls for action. Such guidance documents and recommendations should be approved by the IICB. When needed, CERT-EU should issue calls for action describing urgent security measures which Union ***entities*** are urged to take within a set timeframe. ***The IICB should 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 ▌. The IICB should be supported on technical matters by technical advisory groups composed as the IICB sees fit which should work in close cooperation with CERT-EU, the Union ***entities*** and other stakeholders as necessary. ▌

(16a) Where the IICB finds that a Union entity has not effectively implemented this Regulation or guidance documents, recommendations or calls for action issued under this Regulation, should also be able to, without prejudice to the internal procedures of the Union entity concerned, proceed with compliance measures. The system of compliance measures should be used with a progressive severity, meaning that when the IICB adopts the compliance measures it should start with a reasoned opinion 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.

(16b) The reasoned opinion represents the least severe compliance measure addressing identified gaps with the implementation of this Regulation. It may be followed by guidance to the Union entity to bring its framework, risk-management measures, cybersecurity plans and reporting in compliance with this Regulation, and then by a warning to address identified shortcomings of the Union entity within a specified period. If the shortcomings identified in the warning have not been sufficiently addressed, the IICB should be able to issue a reasoned notification.

(16c) The IICB may further recommend that an audit of a Union entity be carried out. The Union entity may use its internal audit function for this purpose. The IICB could also request that an audit is performed by a third-party audit service, including from a mutually agreed private sector service provider.

(16e) 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. This advisory should be communicated through appropriate secure communication channels.

(16f) To ensure the correct implementation of this Regulation, 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, including suggestions of actions of disciplinary nature, in accordance, in particular, with the rules and procedures laid down in the Staff Regulations and the Conditions of employment of other servants of the European Union.

(17) CERT-EU should have the mission to contribute to the security of the ***ICT*** environment of all Union ***entities***. ***When considering whether to provide technical advice or input on relevant policy matters upon the request of a Union entity, CERT-EU should ensure that this does not impede the fulfilment of its other tasks laid down in this Regulation***. CERT-EU should act as the equivalent of the designated coordinator for the Union ***entities***, for the purpose of coordinated vulnerability disclosure to the European vulnerability ***database*** as referred to in Article ***12*** of Directive ***(EU) 2022/2555***.

▌

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

(20) In supporting operational cybersecurity, CERT-EU should make use of the available expertise of the European Union Agency for Cybersecurity ***(ENISA)*** through structured cooperation as provided for in Regulation (EU) 2019/881 of the European Parliament and of the Council[4]. 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 ***ENISA*** on threat analysis and share its threat landscape report with the Agency on a regular basis.

---

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

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

(21) ***CERT-EU should be able to*** cooperate and exchange information with ***relevant cybersecurity communities*** to foster operational cooperation and to enable the existing networks in realising their full potential in protecting the Union.

▌

(22a) Regulation (EU) 2018/1725[5] applies to any processing of personal data under this Regulation. The processing of personal data could take place in relation to measures adopted in the context of cybersecurity risk management, vulnerability and incident handling, information sharing about incidents, cyber threats and vulnerabilities, and incident response coordination and cooperation. Such measures could require the processing of certain categories of personal data, such as IP addresses, uniform resources locators (URLs), domain names, email addresses, organisational roles of the data subject, time stamps, email subjects or file names. All measures taken under this Regulation should be compliant with the data protection and privacy framework, and the Union entities, CERT-EU and, where relevant the IICB, should take all relevant technical and organisational safeguards to ensure this compliance in an accountable way.

(22b) This Regulation establishes the legal basis for the processing of personal data by Union entities, CERT-EU and, where relevant, by the IICB, for the purpose of performing their tasks and fulfilling their obligations under this Regulation, in accordance with Article 5(1) point (b) Regulation (EU) 2018/1725. CERT-EU may act as processor or controller depending on the task it performs within the meaning of Regulation (EU) 2018/1725.

---

5 *Reference of the EUDPR.*

(22c) ***In certain cases, for the purpose of complying with their obligations under this Regulation to ensure a high level of cybersecurity and in particular in the context of vulnerability and incident handling, it may be necessary for Union entities and CERT-EU to process special categories of personal data as referred to in Article 10(1) of Regulation (EU) 2018/1725. This Regulation establishes the legal basis for the processing of special categories of personal data by Union entities and CERT-EU in accordance with Art. 10(2) (g) of Regulation (EU) 2018/1725. The processing of special categories of personal data under this Regulation should be strictly proportionate to the aim pursued. Subject to the conditions set out under Article 10(2), point (g), of that Regulation, the Union entities and CERT-EU should be able to process such data only to the extent necessary and where explicitly provided for in this Regulation. When processing special categories of personal data, the Union entities and CERT-EU should respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subjects.***

(22d) Pursuant to Article 33 of Regulation (EU) 2018/1725, CERT-EU and Union entities should, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, implement appropriate technical and organisational measures to ensure an appropriate level of security of personal data, such as the provision of restricted access rights on a need-to-know basis, application of audit trail principles, adoption of chain of custody, storage of data at rest in a controlled and auditable environment, and standardised operational procedures, and privacy preserving measures, such as pseudonymisation, or encryption. Those measures should not be implemented in a manner affecting the purposes of incident handling and integrity of evidence. Where Union entities or CERT-EU transfer personal data related to an incident, including special categories of data, to a counterpart or partner for the purposes of this Regulation, such transfers should comply with Regulation (EU) 2018/1725. Where special categories of personal data are transferred to a third party, CERT-EU should ensure that the third party applies personal data protection measures at a level equivalent to Regulation (EU) 2018/1725.

(22e) Personal data processed for the purposes of this Regulation should be retained only for as long as necessary in accordance with Regulation (EU) 2018/1725. Union entities and, where applicable CERT-EU acting as a controller, should define retention periods which should be limited to what is necessary to achieve the specified purposes. In particular in relation to data collected for incident handling, Union entities and CERT-EU should differentiate between personal data that is collected for the detection of a cyber threat in their ICT systems to prevent an incident and personal data that is collected for the mitigation of, response to and recovery from an incident. For the detection of a cyber threat, it is important to take into account the time that a threat actor can remain undetected in a system. For the mitigation of, response to and recovery from an incident, it is important to consider whether the data is necessary to trace and handle a recurrent incident or an incident of similar nature for which a correlation could be demonstrated.

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

(22g) The cybersecurity risk management measures put in place by EUIBAs should include policies aimed at transparency of the source code, where possible and taking into account safeguards for the rights of third parties or EUIBAs. The measures should be proportionate to the risk and are intended to facilitate the analysis of the threats, while not creating obligations to disclose or rights to access third party code beyond the applicable contractual terms.

(23) The handling of information by CERT-EU and the Union ***entities*** should be in line with the ***applicable rules*** on information security. ***The inclusion of human resources*** security ***as a risk management measure should also be in line with the applicable rules***.

(23a) For the purposes of sharing information visible markings are used to indicate that sharing boundaries are to be applied by the recipients of the information based on, in particular, non-disclosure agreements, or informal non-disclosure agreements such as the traffic light protocol or other clear indications by the source. The traffic light protocol is to be understood as a means to provide information about any limitations with regard to the further spreading of information. It is used in almost all computer security incident response teams (CSIRTs) and in some information analysis and sharing centres.

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

(24a) The Regulation reflects and considers that Union entities differ in their size and capacity, including in terms of financial and human resources.

(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. ***That report, with the input of IICB, should evaluate the appropriateness of including network and information systems handling EUCI in scope of this Regulation, in particular in the absence of information security rules common to all Union entities***.

HAVE ADOPTED THIS REGULATION:

Chapter I

GENERAL PROVISIONS

Article 1

Subject-matter

This Regulation lays down ***measures that aim to achieve a high common level of cybersecurity within Union entities with regard to***:

(a) ***the establishment by each Union entity of*** an internal cybersecurity risk management, governance and control framework;

(b) cybersecurity risk management ***,*** reporting ***and information sharing for Union entities***;

(c) the organisation***, functioning*** and operation of ***the Cybersecurity Service*** for the Union institutions, bodies***, offices*** and agencies (CERT-EU)***, as well as*** the organisation***, functioning*** and operation of the Interinstitutional Cybersecurity Board ***(IICB);***

(ca) the monitoring of the implementation of this Regulation.

Article 2

Scope

1. This Regulation applies to ▌ all Union ***entities*** and to ▌ CERT-EU and the ***IICB***.

2. ***This Regulation applies without prejudice to the institutional autonomy pursuant to the Treaties.***

3. ***With the exception of Article 12(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 ***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 ***as defined in*** Article ***6, point (1),*** of Directive ***(EU) 2022/2555***;

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

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

(5) ‘highest level of management’ means a manager, management or coordination and oversight body ***responsible for the functioning of the Union entity concerned,*** at the most senior administrative level, ***with a mandate to adopt or authorise decisions in line with*** the high-level governance arrangements ***of the entity concerned, without prejudice to the formal responsibilities of other levels of management for compliance and risk management in their respective areas of responsibility***;

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

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

(8) ‘major ***incident***’ means 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***;

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

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

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

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

▌

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

▌

▌

Article 3a

Processing of personal data

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

2. ***Where they perform tasks or fulfill obligations pursuant to this Regulation, CERT-EU, the IICB and Union entities shall process and exchange personal data only to the extent necessary and for the sole purpose of performing those tasks or fulfilling those obligations.***

3. The processing of special categories of personal data as referred to in Article 10(1) of Regulation (EU) 2018/1725 shall be considered necessary for reasons of substantial public interest within the meaning of Article 10(2) point (g) of Regulation (EU) 2018/1725. Such data may be processed only to the extent necessary for the implementation of cybersecurity risk management measures referred to in Articles 4 and 5, the provision of services by CERT-EU pursuant to Article 12, for the sharing of incident specific information pursuant to Articles 16(2) and 17(3), the sharing of information pursuant Article 19, the reporting obligations pursuant Article 19, the incident response coordination and cooperation pursuant to Article 21 and management of major incidents pursuant to Article 22 of this Regulation. The data controller shall apply technical measures to prevent the processing of data for other purposes and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subjects.

Chapter II

MEASURES FOR A HIGH COMMON LEVEL OF CYBERSECURITY

Article 3b

Implementation of measures

1. The IICB shall, after consulting the European Union Agency for Cybersecurity (ENISA) and upon receiving guidance from CERT-EU, by ... [eight months after the date of entry into force of this Regulation], issue guidance documents to Union entities for the purpose of carrying out the initial cybersecurity review and the establishment of the framework referred to in article Y, the cybersecurity maturity assessments referred to in Article Z, the cybersecurity risk-management measures referred to in article XY as well as the cybersecurity plan referred to in Article XZ.

2. When implementing articles Y, Z, XY, and XZ, the Union entities shall take into account the guidance documents referred to in paragraph 1 of this article, as well as relevant guidance documents and recommendations adopted in accordance with Articles 10 and 13.

Article 4

Risk management, governance and control ***framework [Y]***

1. Each Union ***entity*** shall establish ***an*** internal cybersecurity risk management, governance and control framework ('the framework') ***following an initial cybersecurity review, such as an audit. The establishment of the framework*** shall be overseen by the ***Union*** entity's highest level of management ***and shall be under its responsibility***. The framework shall be in place by …. ▌ [15 months after the entry into force of this Regulation].

2. The framework shall cover the entirety of the ***unclassified ICT*** environment of the concerned ***Union entity***, including any on-premise ***ICT*** 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 ***ICT environment ("ICT*** environment***")***. The framework shall ***be based on an all-hazard approach.***

2a. The framework shall ensure a high level of cybersecurity. The framework shall lay down internal cybersecurity policies, including objectives and priorities, for the security of network and information systems, and define the roles and responsibilities of staff of the Union entity tasked with ensuring the effective implementation of this Regulation. The framework shall also include mechanisms to measure the effectiveness of the implementation.

2b. ***The framework shall be reviewed on a regular basis, in light of the changing risks, and at least every four years. Where appropriate and upon request of the IICB, a Union entity's framework may be updated following guidance from CERT-EU on incidents identified or possible gaps observed in the implementation of this Regulation.***

3. The highest level of management of each Union ***entity shall be responsible for the implementation and shall oversee*** the compliance of ***its*** organisation with the obligations related to ***the framework***.

3a. ***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. Regardless of possible delegation of its specific obligation, the highest level of management may be held liable for the non-compliance by the entities with the obligations under this Regulation.***

4. Each Union ***entity*** shall have effective mechanisms in place to ensure that an adequate percentage of the ***ICT*** budget is spent on cybersecurity. ***Due account shall be taken of the framework when defining this percentage.***

5. Each Union ***entity*** shall appoint a Local Cybersecurity Officer or an equivalent function who shall act as its single point of contact regarding all aspects of cybersecurity. ***The Local Cybersecurity Officer shall facilitate the implementation of this Regulation and directly 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 certain tasks of Local Cybersecurity Officer with respect to the implementation of this Regulation to CERT-EU on the basis of a service level agreement concluded between that Union entity and CERT-EU, or these tasks may be shared by several Union entities. In case these tasks are delegated to CERT-EU, the IICB shall decide whether the provision of this service shall be part of the baseline services of CERT-EU, taking into account the human and financial resources of the concerned Union entity. Appointed Local Cybersecurity Officers and any subsequent change thereto shall be notified by each Union entity to CERT-EU without undue delay. CERT-EU shall keep the regularly updated list of appointed Local Cybersecurity Officers.***

6. The senior officials within the meaning of Article 29(2) of the Staff Regulations[6] or other officials at equivalent level, of each Union entity, as well as all relevant staff tasked with implementing the cybersecurity risk-management measures and obligations laid down in this Regulation shall follow specific trainings on a regular basis to gain sufficient knowledge and skills in order to apprehend and assess cybersecurity risk and management practices and their impact on the operations of the organisation.

---

[6] ***Regulation No 259/68 of the Council 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.***

Article 6

Cybersecurity maturity assessments ***[Z]***

1. Each Union ***entity shall, by [18 months after entry into force of this Regulation] and*** at least every ***two*** years ***thereafter carry out a cybersecurity maturity assessment*** incorporating all the elements of their ***ICT*** environment as described in Article ***Y***.

2. The cybersecurity maturity assessments shall, where appropriate, be carried out with the assistance of a specialised third-party.

3. Union entities with similar structures may cooperate in carrying out maturity assessments for their respective entity.

4. Upon request of the IICB, and with the explicit consent of the Union entity concerned, the results of a cybersecurity maturity assessment may be discussed within the IICB or within the informal group of Local Cybersecurity Officers with a view to learning from experiences and sharing best practices.

Article 5

Cybersecurity ***risk management measures [XY]***

1. ***Without undue delay and no later than [20 months after the entry into force of this Regulation],*** each Union ***entity shall, under the oversight of its highest level of management, ensure that appropriate and proportionate technical, operational and organisational measures are taken to manage*** the risks identified under the framework***, and to prevent or minimise the impact of incidents. Taking into account the state of the art and, where applicable, relevant European and international standards, those measures*** shall ***ensure a level of security of network and information systems across the entirety of the ICT environment commensurate to the risks. When assessing the proportionality of those measures, due account*** shall ***be taken of the degree of the Union entity's exposure to risks, its size, the likelihood of occurrence of incidents and their severity, including their societal, economic and interinstitutional impact***.

1a. Union entities shall address at least the following domains in the implementation of the cyber security risk-management measures:

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

(b) risk analysis and information system security policies;

(c) policy objectives regarding the use of cloud computing services as defined in Article 6, point (30), of Directive (EU) 2022/2555;

(d) cybersecurity audit, where appropriate, which may include a risk, vulnerability and threat assessment, and penetration-test carried out by a trusted private provider on a regular basis;

(e) implement recommendations of audits referred to in (d) through cybersecurity and policy updates;

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

(g) asset management, including ICT asset inventory and ICT network cartography;

(h) human resources security and access control;

(i) operations security;

(j) communications security;

(k) system acquisition, development, maintenance, including policies on vulnerability handling and disclosure.

(l) where possible policies on transparency of source code;

(l) supply chain security including security related aspects concerning the relationships between each Union entity and its direct suppliers or service providers. 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;

(m) incident handling and cooperation with CERT-EU, such as the maintenance of security monitoring and logging;

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

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

2a. Union entities shall address at least the following specific cybersecurity risk management measures:

(a) technical arrangements to enable and sustain teleworking;

(b) concrete steps for moving towards Zero Trust principles;

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

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

(e) secured voice, video and text communications, and secured emergency communications systems within the Union entity, where appropriate;

(f) proactive measures for detection and removal of malware and spyware.

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

(i) the establishment and adoption of training programmes on cybersecurity commensurate to the prescribed tasks and expected capabilities for the highest level of management and staff of the Union entity tasked with ensuring the effective implementation of this Regulation;

(h) regular cybersecurity training of staff members;

(j) participation in interconnectivity risk analyses between the Union entities where relevant;

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

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

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

Article 7

Cybersecurity plans ***(XZ)***

1. Following the conclusions derived from the ***cybersecurity*** maturity assessment ***referred to in Article Z*** and considering the assets and risks identified ***in the framework as well as the cybersecurity risk-management measures in*** Article ***XY***, the highest level of management of each Union ***entity*** shall approve a cybersecurity plan without undue delay ***and no later than 24 months after the entry into force of this Regulation. The cybersecurity*** plan shall aim at increasing the overall cybersecurity of the ***Union*** entity and shall thereby contribute to the ▌ enhancement of a high common level of cybersecurity ***within the Union entities. The cybersecurity*** plan shall at least include the ***cybersecurity risk-management*** measures ***referred to in article XY. The cybersecurity*** plan shall be revised at least every ***two*** years, ***or when necessary,*** following the maturity assessments carried out pursuant to Article ***Z or any substantial review of the framework***.

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

4. Upon completion of the cybersecurity plan, the Union entity shall submit it to the IICB.

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 ***and supporting*** the implementation of this Regulation by the Union ***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 European Commission;

(iv) the Council of the European Union;

(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 Cybersecurity Industrial, Technology and Research Competence Centre;

(xiii) the European Union Agency for Cybersecurity;

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

(xv) the European Union Agency for the Space Programme.

b) ▌three representatives ***designated*** by the Union Agencies Network (EUAN) upon a proposal of its ICT Advisory Committee to represent the interests of the agencies***, offices*** and bodies that run their own ***ITC*** environment, ***other than those referred to in paragraph 3, point (a).***

▌

▌

▌

The Union entities represented in the IICB shall aim to achieve gender balance among the designated representatives.

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

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

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

5. The IICB shall designate a chair, in accordance with its internal rules of procedure, from among its members for a period of ***three*** 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, ***or*** at the request of CERT-EU or at the request of any of its members.

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

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

▌

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

11. The representatives nominated by the EUAN ▌ shall relay the IICB's decisions to the ***members of the EUAN. Any member of EUAN*** shall be entitled to raise with ***those*** representatives or the chair of the IICB any matter which it considers should be brought to the IICB's attention.

▌

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

13a. The IICB shall submit a report to the European Parliament and to the Council every 12 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 18 of Directive [proposal NIS 2].

Article 10

Tasks of the IICB

When exercising its responsibilities, the IICB shall in particular:

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

(a) ***effectively monitor and supervise the application of this Regulation and support the Union entities to strengthen their cybersecurity; to this end, the IICB may request ad-hoc reports from CERT-EU and Union entities***;

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

(ac) establish the methodology and organisational aspects for the conducting of voluntary peer reviews by Union entities, with a view to learning from shared experiences, strengthening mutual trust, achieving a high common level of cybersecurity, as well as enhancing Union entities' cybersecurity capabilities. The peer reviews shall be conducted by cybersecurity experts designated by a Union entity different form the Union entity being reviewed. The methodology shall be based on Article 19 of Directive (EU) 2022/2555, where appropriate adapted to the Union entity.

(b) approve, on the basis of a proposal ***submitted by*** 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 ***agreements*** or contracts between CERT-EU and other entities pursuant to Article 17;

(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;

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

(k) receive and assess documents and reports submitted by the Union entities under this Regulation, such as cybersecurity maturity assessments;

(ic) facilitate the establishment of an informal group of Local Cybersecurity Officers of all Union entities, supported by ENISA, with the aim of exchanging best practices and information in relation to the implementation of this Regulation;

(id) taking into account the information on the identified risks and lessons learnt provided by CERT-EU, monitor the adequacy of interconnectivity arrangements among the Union entities' ICT environments and advise on possible improvements;

(ie) develop a cyber-crisis management plan with a view to supporting the coordinated management of major incidents at an operational level affecting Union entities and to contributing to the regular exchange of relevant information, in particular with regard to the impacts and severity of, and the possible ways of mitigating the effects of major incidents;

(ih) coordinate the adoption of individual Union entities' cyber crisis management plans referred to in Article 7(2a);

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

Article 11

Compliance

1. The IICB shall***, in accordance with 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 ***entities***. The IICB ***may request information or documentation necessary for that purpose from the Union entities. For the purpose of adopting compliance measures*** under this ***article, where the entity is directly represented in the IICB, the Union entity concerned shall not have voting rights***.

(-a) Where the IICB finds that a Union entity has not effectively implemented this Regulation or guidance documents, recommendations or calls for action issued under this Regulation, it may, without prejudice to the internal procedures of the Union entity concerned, and after having given the opportunity to the Union entity concerned to present its observations;

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

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

(c) issue a warning ***to address identified shortcomings within a specified period, including recommendations to amend measures adopted by the Union entity pursuant to this Regulation***; where necessary in view of a compelling cybersecurity risk, the audience of the warning shall be restricted appropriately;

(d) issue a reasoned notification to the concerned Union entity, in case that shortcomings identified in a warning issued pursuant to point (c) were not sufficiently addressed within the specified period;

(e) issue:

(i) a recommendation for an audit to be carried out or;

(ii) a request that an audit be performed by a third party audit service;

(f) if applicable, within the remit of its mandate, inform the Court of Auditors of the alleged non-compliance.

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

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

4. Where the IICB has adopted measures under paragraph 2 points (a) - (g), the Union entity concerned shall provide details of the measures and actions taken to address the alleged shortcomings identified by the IICB. The Union entity shall submit those details within a reasonable period to be agreed with the IICB.

3. Where the IICB considers that there is continuous non-compliance with 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 Union entity concerned to take the appropriate actions, including suggestions of actions of disciplinary nature, in accordance, in particular, with the rules and procedures 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 Union entity concerned.

2. Where Union entities notify that they are unable to meet the deadlines set out in Articles 4(1) and 5(1), the IICB may, in duly justified cases, taking into account the size of the entity, authorise the extension of the deadlines.

Chapter IV

CERT-EU

Article 12

CERT-EU mission and tasks

1. ***CERT-EU's mission*** shall be to contribute to the security of the unclassified ***ICT*** environment of all Union ***entities*** by advising them on cybersecurity, by helping them to prevent, detect, ***handle***, mitigate***, respond to and recover from*** incidents and by acting as their cybersecurity information exchange and incident response coordination hub.

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

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

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

(b) ***offer standard CSIRT 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) ▌ on the ***basis of the information referred to in paragraph 1a,*** contribute to the EU cyber situational awareness ***in close cooperation with ENISA. Such information shall be shared with the IICB, as well as the CSIRTs Network and EU-INTCEN where appropriate and applicable, and under appropriate confidentiality conditions***;

(x) coordination of the handling of major incidents;

(f) act as the equivalent of the designated coordinator for the Union entities, as referred to in Article 6 of Directive [proposal NIS 2].

(ef) provide, upon the request of a Union entity, proactive non-intrusive scanning of publicly accessible network and information systems of a Union entity;

3. CERT-EU ***may, in accordance with Art. 16 or Art. 17 as appropriate, cooperate with relevant cybersecurity communities within the Union and its Member States***, including in the following areas:

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

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

(c) cyber threat intelligence, including situational awareness;

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

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

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

   (a) services that support the cybersecurity of Union ***entities' ICT*** environment, other than those referred to in paragraph 2, on the basis of service level agreements and subject to available resources***, in particular a broad-spectrum network monitoring, including first-line 24/7 monitoring for high-severity threats.***

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

(x) upon request, a proactive scanning of the network and information systems of the Union entity concerned to detect vulnerabilities with a potential significant impact;

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

CERT-EU may exceptionally enter into service level agreements with entities other than the Union entities with the prior approval of the IICB.

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

7. CERT-EU may provide assistance to Union ***entities regarding incidents in network and information systems handling EUCI*** if it is explicitly requested to do so by the ***Union entities*** concerned ***in accordance with their respective procedures. The provision of assistance by CERT-EU under this paragraph shall be without prejudice to applicable rules concerning the protection of classified information***.

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

7b. CERT-EU shall contribute, with a high level of confidentiality and reliability, via the appropriate cooperation mechanisms and reporting lines, relevant and anonymised information about the major incidents and the way they were dealt with. The information shall also be included in the report referenced in Article 9 (13a).

11. CERT-EU shall, in cooperation with the European Data Protection Supervisor, support the Union entities concerned when addressing incidents resulting in personal data breaches, without prejudice to the competence and tasks of EDPS as a supervisory authority under Regulation EU 2018/1725.

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

Article 13

Guidance documents, recommendations and calls for action

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

(a) calls for action describing urgent security measures that Union ***entities*** are urged to take within a set timeframe. ***Without undue delay after receiving the call for action the concerned Union entity shall inform CERT-EU of how those measures were applied***;

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

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

1a. Guidance documents and recommendations may include:

(-a) common methodologies and a model for assessing the cybersecurity maturity of the Union entities, including the corresponding scales or key performance indicators (KPI), serving as reference in support of continuous cybersecurity improvement across the Union entities and facilitating the prioritisation of cybersecurity domains and measures taking into account entities' cybersecurity posture;

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

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

(c) where appropriate, the use of common technology, architecture***, open-source*** and associated best practices with the aim of achieving interoperability and common standards***, including a coordinated approach to supply chain security***;

(ca) where appropriate, information to facilitate the use of common procurement instruments for purchasing of relevant cybersecurity services and products from third party suppliers;

(cb) information sharing arrangements referred to in Article 19.

Article 14

Head of CERT-EU

1. The Commission, after obtaining the approval of a majority of two thirds of the IICB members, shall appoint the head of CERT-EU. The IICB shall be consulted at all stages of the procedure prior to the appointment of the head of CERT-EU, in particular in drafting vacancy notices, examining applications and appointing selection boards in relation to that post. The selection procedure, including the final short list of candidates among which the Head of Cert-EU is chosen, shall ensure fair representation of each gender taking account of the applications submitted.

2. The Head of CERT-EU shall be responsible for the proper functioning of CERT-EU, acting within its remit under the direction of the IICB. He or she shall report regularly to the IICB Chair and submit ad-hoc reports to the IICB upon its request.

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 74(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, CERT-EU 's service catalogue proposal and 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 CERT-EU's service catalogue, the Head of CERT-EU shall take into account the resources allocated to CERT-EU.

5. The Head of CERT-EU shall ▌ submit reports ***at least once a year*** to the IICB and the IICB Chair on the ***activities and*** performance of CERT-EU ***during the reference period, including on the*** implementation of the budget, service level agreements and written agreements entered into, cooperation with counterparts and partners, and missions undertaken by staff, including the reports referred to in Article ***10. Those reports shall include the work programme for the next period, financial planning of revenue and expenditure, including staffing, planned updates of CERT-EU's service catalogue and an assessment of the expected impact that such updates may have in terms of financial and human resources***.

Article 15

Financial and staffing matters

1. ***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 multiannual financial framework established in accordance with Article 312 TFEU to allow for appropriate action to be taken. The evaluation shall include the possibility to establish the CERT-EU as a Union office.***

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

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

4. Union ***entities*** other than those referred to in paragraph 3 shall make an annual financial contribution to CERT-EU to cover the services provided by CERT-EU pursuant to that paragraph 3. The respective contributions shall be based on orientations given by the IICB and agreed between each entity and CERT-EU in service level agreements. The contributions shall represent a fair and proportionate share of the total costs of services provided. They shall be received by the distinct budget line referred to in paragraph 3 as assigned revenue as provided for in Article 21(3), point (c) of Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council[7].

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

[7] 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).

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, CSIRTs referred to in Article 9 of Directive [proposal NIS 2], and/or where applicable national competent authorities*** and single points of contact referred to in Article 8 of Directive ***(EU) 2022/2555***, on cyber threats, vulnerabilities**,** ▌ incidents, ***near misses,*** possible countermeasures ***as well as best practices*** and on all matters relevant for improving the protection of the ***ICT*** environments of Union ***entities***, including through the CSIRTs network referred to in Article ***15 of Directive (EU) 2022/2555. CERT-EU shall support the Commission in the EU-CyCLONe referred to in Article 16*** of Directive ***(EU) 2022/2555 on coordinated management of large-scale cybersecurity incidents and crises***.

1a. ***In alignment with paragraph 1, CERT-EU shall, without delay, notify any relevant national counterparts, when it becomes aware of significant incidents occurring within the territory of that Member State***.

2. ***CERT-EU shall, without undue delay, provided that personal data is protected in accordance with applicable Union data protection law, exchange*** incident-specific information with national counterparts in the Member States ***relevant*** to facilitate detection of similar cyber threats or incidents***, or to contribute to the analysis of an incident,*** without the ***authorisation*** of the ***Union entity affected.*** CERT-EU ***shall not*** exchange incident-specific information which reveals the identity of the target of the cybersecurity incident ***unless***:

2a. ***there is consent of the affected Union entity and in compliance with Union personal data protection law;***

2b. the affected Union entity has already made public that it was affected;

2c. there is no consent of the affected Union entity, but the disclosure of the identity of the affected Union entity would increase the probability that incidents elsewhere will be avoided or mitigated. Such decisions require the approval of the Head of CERT-EU. Prior to issuing such a decision CERT-EU shall contact the concerned Union entity in writing, explicitly explaining how disclosing its identity would help to avoid or mitigate incidents elsewhere. The Head of CERT-EU shall provide the explanation and explicitly request the entity to state whether it consents within a defined timeframe. The Head of CERT-EU shall also clarify to the entity that, in light of the explanation provided, he or she reserves the right to disclose the information even in case of lack of consent. The affected Union entity shall be informed before the information is disclosed.

Article 17

Cooperation of CERT-EU with ***other*** counterparts

1. CERT-EU may cooperate with ***counterparts in the European Union other than those mentioned in Article 16, that are subject to Union cybersecurity requirements***, 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, ***CERT-EU shall seek prior approval from the IICB on a case-by-case basis. CERT-EU shall inform any relevant*** national counterparts ***referred to in Article 16(1), in a*** Member ***State in which the counterpart is located, when CERT-EU establishes cooperation with such counterparts. Where appropriate and relevant, such cooperation and the conditions thereof, including regarding cybersecurity, data protection and information handling***, shall ***be defined in specific confidentiality arrangements such as contracts or administrative arrangements.***

The confidentiality arrangements shall not require prior approval ***by the IICB, but the chair of the IICB shall be informed. In case of urgent and imminent need to exchange cybersecurity information in the interest of the EU entities or another party, CERT-EU may do so with an entity, whose specific competence, capacity and expertise are justifiably required to assist with such an urgent and imminent need, even if it does not have a prior confidentiality arrangement in place; in these cases, CERT-EU will immediately inform the Chair of*** the IICB***, and it will report to the IICB via regular reports or meetings***.

2. CERT-EU may cooperate with other partners, such as commercial entities, ***including industry sector-specific entities,*** international organisations, non-European Union national entities or individual experts, to gather information on general and specific cyber threats, ***near misses,*** vulnerabilities and possible countermeasures. For wider cooperation with such partners, CERT-EU shall seek prior approval from the IICB ***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*** affected by an incident, provide information related to the ***specific*** incident to partners ***referred to in paragraphs 1 and 2 solely for the purpose of contributing*** to its analysis.

Chapter V
COOPERATION AND REPORTING OBLIGATIONS

Article 18
Information handling

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

2. The provisions of Regulation (EC) No 1049/2001 of the European Parliament and the Council[8] shall apply with regard to requests for public access to documents held by CERT-EU, including the obligation under that Regulation to consult other Union ***entities or, where relevant, Member States,*** whenever a request concerns their documents.

[8] 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).

▌

4. The handling of information by CERT-EU and Union ***entities*** shall be in line with the ***applicable*** rules ▌ on information security▌ .

▌

5a. Union entities shall upon request share information with the European Parliament and the Council on the completion of cybersecurity plans.

5b. Where relevant, the IICB, or where applicable CERT-EU, shall upon request share guidance documents, recommendations and calls for action with the European Parliament and the Council.

Article 19

Cybersecurity information sharing arrangements

-1. Union entities may voluntarily notify and provide information to CERT-EU on cyber threats, incidents, near misses and vulnerabilities that affect them. CERT-EU shall ensure that efficient means of communication, with a high level of traceability, confidentiality and reliability, are available for the purpose of facilitating information sharing with the Union entities. When processing notifications, CERT-EU may prioritise the processing of mandatory notifications over voluntary notifications. Without prejudice to Art. 11, voluntary notification shall not result in the imposition of any additional obligations upon the reporting Union entity to which it would not have been subject had it not submitted the notification.

1. To ***perform its mission and tasks as defined in Article 12, CERT-EU*** may request Union ***entities*** to provide it with information from their respective ***ICT*** system inventories***, including information relating to cyber threats, near misses, vulnerabilities, indicators of compromise, cybersecurity alerts and recommendations regarding configuration of cybersecurity tools to detect cyber incidents. The requested Union entity*** shall transmit the requested information, and any subsequent updates thereto, without undue delay.

▌

3. CERT-EU may only exchange incident-specific information ***with the Union entities*** which reveals the identity of the Union ***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.***

4. The sharing obligations shall not extend to:

a. EUCI;

b. information ***the further distribution of which has been excluded by means of a visible marking unless the sharing thereof with CERT-EU has been explicitly allowed***.

Article 20

Reporting obligations

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

-1a. 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;

-1b. it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

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

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

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

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

(iii) applied and ongoing mitigation measures;

(iv) where applicable, the cross-border or cross-entity 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.

2a. All Union entities shall inform, without undue delay and in any event within 24 hours after becoming aware, that a significant incident has occurred, any relevant national counterparts referred to in Article 16(1) in the Member State where it is located.

3. The Union entities shall notify, inter alia, any information enabling CERT-EU to determine any cross-entities impact, impact on the hosting Member State or cross-border impact following a significant incident. Without prejudice to Article 11, the mere act of notification shall not subject the Union entity to increased liability;

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

5. Where a significant incident or significant cyber threat affects a network and information system, or a component of a Union entity's ICT environment that is knowingly connected with another Union entity's ICT environment, CERT-EU shall issue a relevant cybersecurity alert;

6. The Union entities, upon the request of CERT-EU shall without undue delay, provide CERT-EU with digital information created by the use of electronic devices involved in their respective incidents. CERT-EU may further clarify which types of such information it requires for situational awareness and incident response.

3. CERT-EU shall submit to ***the IICB,*** ENISA, ***the EU INTCEN and the CSIRTs Network every three months*** a summary report including ***anonymized*** and aggregated data on significant ***incidents,*** cyber threats, ***incidents, near misses and*** vulnerabilities ***in accordance with Article 19*** and significant incidents notified in accordance with paragraph 1. ***That report shall constitute an input to the biennial report on the state of cybersecurity in the Union under Article 18 of Directive 2022/2555.***

8. The IICB ***shall, by [6 months after the date of entry into force of this Regulation],*** issue guidance documents or recommendations ***further specifying*** the modalities***, format*** and content of the ***reporting. When preparing such guidance documents or recommendations, the IICB shall take into account the specifications made by any implementing acts adopted by the Commission specifying the type of information, the format and the procedure of a*** notification ***submitted pursuant to Article 23(11) of Directive (EU) 2022/2555***. CERT-EU shall disseminate the appropriate technical details to enable proactive detection, incident response or mitigating measures by Union ***entities***.

9. The ***reporting*** obligations shall not extend to:

a. EUCI;

b. information ***the further distribution of which has been excluded by means of a visible marking unless the sharing thereof with CERT-EU has been explicitly allowed***.

Article 21

Incident response coordination and cooperation ▌

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

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

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

2. CERT-EU***, where relevant in close cooperation with ENISA*** shall facilitate coordination among Union ***entities*** on incident response, including:

   (a) contribution to consistent external communication;

(b) mutual ***support, such as sharing information pertinent to Union entities, or providing*** assistance***, when relevant directly on-site***;

(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 entities*** regarding situational awareness of cyber threats, vulnerabilities***, near misses*** and incidents ***as well as sharing relevant developments in the field of cybersecurity***.

4. The IICB shall***, by [12 months after the date of entry into force of this Regulation], on the basis of a proposal from CERT-EU, adopt*** 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 ***without undue delay***.

4a. Following a specific request from the Member State and with the approval of the concerned Union entities, CERT-EU may also call on experts from the list referred to in article 22 paragraph 2 for contributing to the response to a major incident which has an impact in a Member State, or a large-scale cybersecurity incident as defined in Article 6, point (7), of Directive (EU) 2022/2555 in line with article 15.3 (g) of Directive EU 2022/2555. Specific rules on access to and use of technical experts from Union entities shall be approved by IICB at the proposal of CERT-EU.

Article 22

Management of major ***incidents***

-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, pursuant to Article 10, first subparagraph, point m, develop a cyber crisis management plan based on activities detailed in Article 21(2), in close cooperation with CERT-EU and ENISA. That cyber crisis management plan shall include, at least, the following elements:

(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 major incident severity and crisis triggering points;

(d) regular exercises;

(e) secure communication channels to be used.

1a. The Commission representative in the IICB shall, subject to the conditions laid down in the cyber crisis management plan and without prejudice to Article 16(2), first subparagraph, of Directive (EU) 2022/2555, be the point of contact for the sharing of relevant information in relation to major incidents with EU-CyCLONe.

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

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

Chapter VI
FINAL PROVISIONS

Article 23
Initial budgetary reallocation

In order to ensure proper and stable functioning of CERT-EU, the Commission ***may*** propose the reallocation of staff and financial resources ▌ to the Commission budget ***for use in CERT-EU operations***. The reallocation shall be effective at the same time as the first budget adopted following the entry into force of this Regulation.

Article 24

Review

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

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

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

3. The Commission shall evaluate the functioning of this Regulation and report to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions no ***later*** than five years after the date of entry into force. ***The Commission shall also evaluate the appropriateness of including network and information systems handling EU Classified Information (EUCI) within the scope of this Regulation, taking into account other Union legislative acts applicable to those systems. The report shall be accompanied, where necessary, by a legislative proposal.***

Article 25

Entry into force

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

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

Done at **...**,

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