EUROPEAN UNION

THE EUROPEAN PARLIAMENT **THE COUNCIL**

Strasbourg, 13 December 2023
(OR. en)

2022/0085 (COD)
LEX 2289

PE-CONS 57/1/23
REV 1

CYBER 215
TELECOM 267
INST 341
CSC 445
CSCI 163
INF 206
FIN 928
BUDGET 27
DATAPROTECT 236
CODEC 1607

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

REGULATION (EU, Euratom) 2023/…
OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 13 December 2023

laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union

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[1],

[1] Position of the European Parliament of 21 November 2023 (not yet published in the Official Journal) and decision of the Council of 8 December 2023.

Whereas:

(1) In the digital age, information and communication technology is a cornerstone of an open, efficient and independent European administration. Evolving technology and the increased complexity and interconnectedness of digital systems amplify cybersecurity risks, making Union entities more vulnerable to cyber threats and incidents, which poses a threat to their business continuity and capacity to secure their data. While the increased use of cloud services, the ubiquitous use of information and communication technology (ICT), the high level of digitalisation, remote work and evolving technology and connectivity are core features of all activities of Union 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 threat actors 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) Union entities' ICT environments have interdependencies and integrated data flows, and their users collaborate closely. That interconnection means that any disruption, even when initially confined to a single Union entity, can have cascading effects more broadly, potentially resulting in far-reaching and long-lasting negative impacts on other Union entities. In addition, certain Union entities' ICT environments are connected with Member States' ICT environments, causing an incident in a Union entity to pose a cybersecurity risk to the Member States' ICT environments and vice versa. The sharing of incident-specific information may facilitate the detection of similar cyber threats or incidents affecting Member States.

(4) Union entities are attractive targets that 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 vary significantly across those entities. It is thus necessary for the functioning of the Union entities that they achieve a high common level of cybersecurity through the implementation of cybersecurity measures commensurate with identified cybersecurity risks, information exchange and collaboration.

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

(6) To reach a high common level of cybersecurity, it is necessary that each Union entity establish an internal cybersecurity risk-management, governance and control framework (the 'Framework'), which ensures an effective and prudent management of all cybersecurity risks, and takes account of business continuity and crisis management. The Framework should establish cybersecurity policies, including objectives 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-hazards approach which aims to protect network and information systems and the physical environment of those systems from events such as theft, fire, flooding, telecommunication or power failures, or unauthorised physical access and damage to, and interference with, a 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.

[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).

(7) To manage the cybersecurity risks identified under the Framework, each Union entity should take appropriate and proportionate technical, operational and organisational measures. Those measures should address the domains and cybersecurity risk-management measures provided for in this Regulation to strengthen the cybersecurity of each Union entity.

(8) The assets and cybersecurity risks identified in the Framework as well as conclusions derived from regular cybersecurity maturity assessments should be reflected in a cybersecurity plan established by each Union entity. The cybersecurity plan should include the adopted cybersecurity risk-management measures.

(9) As ensuring cybersecurity is a continuous process, the suitability and effectiveness of the measures taken pursuant to this Regulation should be regularly revised in light of the changing cybersecurity risks, assets and cybersecurity 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 every two years, or more frequently where necessary, following the cybersecurity maturity assessments or any substantial review of the Framework.

(10) The cybersecurity risk-management measures put in place by Union entities should include policies aiming, where possible, to render the source code transparent, taking into account safeguards for the rights of third parties or Union entities. Those policies should be proportionate to the cybersecurity risk and are intended to facilitate the analysis of cyber threats, while not creating obligations to disclose or rights to access third-party code beyond the applicable contractual terms.

(11) 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.

(12) The differences between Union entities require flexibility in the implementation of this Regulation. The measures for a high common level of cybersecurity provided for in this Regulation 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 and should adopt their own cybersecurity risk-management measures and cybersecurity plans. When implementing such measures, due account should be taken of existing synergies 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 efficient information exchange and cooperation among Union entities and between Union entities and Member State counterparts.

(13) In the interest of optimising the use of resources, this Regulation should provide for the possibility for two or more Union entities with similar structures to cooperate in carrying out the cybersecurity maturity assessments for their respective entities.

(14) In order to avoid imposing a disproportionate financial and administrative burden on Union entities, the cybersecurity risk-management requirements should be proportionate to the cybersecurity risk posed to the network and information systems 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 cybersecurity maturity assessment should evaluate whether the Union entity's cybersecurity spending is proportionate to the cybersecurity risks that it faces. Without prejudice to the rules relating to the Union's annual budget under the Treaties, in its proposal for the first annual 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.

(15) A high common level of cybersecurity requires cybersecurity to come under the oversight of the highest level of management of each Union entity. The Union entity's highest level of management should be responsible for the implementation of this Regulation, including for the establishment of the Framework, the taking of the cybersecurity risk-management measures and the approval of the cybersecurity plan. Addressing the cybersecurity culture, namely the daily practice of cybersecurity, is an integral part of the Framework and the corresponding cybersecurity risk-management measures in all Union entities.

(16) The security of network and information systems handling EU classified information (EUCI) is essential. Union entities that handle 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 comply with 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, the Computer Emergency Response Team for the EU institutions, bodies and agencies (CERT-EU) should be able to provide assistance to that Union entity in relation to incidents in classified ICT environments.

(17) Union entities should assess cybersecurity 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 guidelines or recommendations issued by CERT-EU. When establishing 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 cybersecurity risk assessments and recommendations issued by the Cooperation Group established pursuant to Article 14 of Directive (EU) 2022/2555, such as the EU coordinated risk assessment of the cybersecurity of 5G networks and the EU toolbox on 5G cybersecurity. In addition, taking into account the cyber threat landscape and the importance of building up cyber resilience for the Union entities, the certification of relevant ICT products, ICT services and ICT processes could be required under specific European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881 of the European Parliament and of the Council[1].

[1] 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).

(18) In May 2011, the Secretaries-General of the Union institutions and bodies decided to establish a pre-configuration team for 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 Commission Taskforce with an interinstitutional mandate. In December 2017, the Union institutions and bodies concluded an Interinstitutional arrangement on the organisation and operation of CERT-EU[1]. This Regulation should provide for a comprehensive set of rules on the organisation, functioning and operation of CERT-EU. The provisions of this Regulation prevail over the provisions of the Interinstitutional arrangement on the organisation and operation of CERT-EU that was concluded in December 2017.

(19) CERT-EU should be renamed Cybersecurity Service for the Union institutions, bodies, offices and agencies, but it should keep the short name CERT-EU because of name recognition.

---

[1] Arrangement between the European Parliament, the European Council, the Council of the European Union, the European Commission, the Court of Justice of the European Union, the European Central Bank, the European Court of Auditors, the European External Action Service, the European Economic and Social Committee, the European Committee of the Regions and the European Investment Bank on the organisation and operation of a computer emergency response team for the Union's institutions, bodies and agencies (CERT-EU) (OJ C 12, 13.1.2018, p. 1).

(20) In addition to giving CERT-EU more tasks and an expanded role, this Regulation establishes the Interinstitutional Cybersecurity Board (IICB) in order to facilitate a high common level of cybersecurity among Union entities. The IICB should have an exclusive role in monitoring and supporting the implementation of this Regulation by the Union entities and in supervising the implementation of general priorities and objectives of, and providing strategic direction to, CERT-EU. The IICB should therefore ensure representation of the Union institutions and should include representatives of bodies, offices and agencies of the Union through the EU Agencies Network (EUAN). The organisation and functioning of the IICB should be further regulated by means of internal rules of procedure, which 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 the IICB to have strategic discussion and provide strategic guidance to the IICB. Furthermore, the IICB should be able to establish an executive committee to assist in its work and to delegate some of its tasks and powers to it, in particular 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, arrangements for service level agreements, assessments of documents and reports submitted by the Union entities to the IICB pursuant to this Regulation or tasks related to the preparation of decisions on compliance measures issued by the IICB and to monitoring their implementation. The IICB should lay down the rules of procedure of the executive committee, including its tasks and powers.

(21) The IICB aims to support Union entities in elevating their respective cybersecurity postures through the implementation of 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 for and other aspects of voluntary peer reviews, and facilitate the establishment of an informal group of local cybersecurity officers, supported by the European Union Agency for Cybersecurity (ENISA), with the aim of exchanging best practices and information in relation to the implementation of this Regulation.

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

(23) The IICB should monitor compliance with this Regulation as well as the implementation of guidelines and recommendations, and calls for action. The IICB should be supported on technical matters by technical advisory groups composed as the IICB sees fit. Those technical advisory groups should work in close cooperation with CERT-EU, the Union entities and other stakeholders as necessary.

(24) Where the IICB finds that a Union entity has not effectively implemented this Regulation or the guidelines, recommendations or calls for action issued pursuant thereto, the IICB should be able, without prejudice to the internal procedures of the Union entity concerned, to proceed with compliance measures. The IICB should apply compliance measures progressively – in other words, the IICB should first adopt the least severe measure, namely a reasoned opinion, and only if necessary increasingly severe measures, culminating in the most severe measure, namely a recommendation of a temporary suspension of data flows to the Union entity concerned. Such a recommendation should be applied only in exceptional cases of long-term, deliberate, repetitive or serious infringements of this Regulation by the Union entity concerned.

(25) The reasoned opinion represents the least severe compliance measure addressing observed gaps in the implementation of this Regulation. The IICB should be able to follow up a reasoned opinion with guidance to assist the Union entity in ensuring that its Framework, cybersecurity risk-management measures, cybersecurity plan and reporting comply 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.

(26) The IICB should be able to recommend that an audit of a Union entity be carried out. The Union entity should be able to use its internal audit function for that purpose. The IICB should also be able to request that an audit be performed by a third-party audit service, including from a mutually agreed private-sector service provider.

(27) In exceptional cases of long-term, deliberate, repetitive or serious infringements of this Regulation by a Union entity, the IICB should be able to recommend, as a last resort, to all Member States and Union entities, a temporary suspension of data flows to the Union entity, to be effective until the Union entity has brought the infringement to an end. Such a recommendation should be communicated by means of appropriate and secure communication channels.

(28) To ensure the correct implementation of this Regulation, the IICB should, if it considers that a persistent infringement of this Regulation by a Union entity has been caused directly by the actions or omissions of a member of its staff, including at the highest level of management, request the Union entity concerned to take appropriate action, including requesting it to consider taking action of a disciplinary nature, in accordance with the rules and procedures laid down in the Staff Regulations of Officials of the European Union and the Conditions of Employment of Other Servants of the Union, laid down in Council Regulation (EEC, Euratom, ECSC) No 259/68[1] (the 'Staff Regulations') and any other applicable rules and procedures.

(29) CERT-EU should 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 is no obstacle to carrying out the other tasks conferred on it pursuant to this Regulation. CERT-EU should act on the part of Union entities as the equivalent of the coordinator designated for the purposes of coordinated vulnerability disclosure pursuant to Article 12(1) of Directive (EU) 2022/2555.

---

[1] Regulation (EEC, Euratom, ECSC) 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 and instituting special measures temporarily applicable to officials of the Commission (OJ L 56, 4.3.1968, p. 1).

(30) CERT-EU should support the implementation of measures for a high common level of cybersecurity by means of proposals for guidelines and recommendations to the IICB or by issuing calls for action. Such guidelines 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 guidelines or for a recommendation, or a call for action.

(31) 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 established pursuant to Article 15 of that Directive. Moreover, in line with Commission Recommendation (EU) 2017/1584[1], CERT-EU should cooperate and coordinate a 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 Member State counterparts. CERT-EU should also collaborate with other public as well as private counterparts, including the North Atlantic Treaty Organization, subject to prior approval by the IICB.

[1] 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).

(32) In supporting operational cybersecurity, CERT-EU should make use of the available expertise of ENISA through structured cooperation as provided for in Regulation (EU) 2019/881. 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 ENISA on cyber threat analysis and share its threat landscape report with ENISA on a regular basis.

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

(34) As the services and tasks of CERT-EU are in the interest of 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.

(35) 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 incidents, Union entities should be able to notify CERT-EU of incidents, cyber threats, vulnerabilities and near misses and share appropriate technical details that enable detection or mitigation of, as well as response to, similar incidents, cyber threats, vulnerabilities and near misses in other Union entities. Following the same approach as in Directive (EU) 2022/2555, Union entities should be required to submit an early warning to CERT-EU within 24 hours of becoming aware of a significant incident. 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 entities' ICT environments and the Union entities' counterparts' ICT environments against similar incidents.

(36) This Regulation lays down a multiple-stage approach to the reporting of significant incidents in order to strike the right balance between, on the one hand, swift reporting that helps mitigate the potential spread of significant incidents and allows Union entities to seek assistance and, on the other, in-depth reporting that draws valuable lessons from individual incidents and improves over time the cyber resilience of individual Union entities and contributes to increasing their overall cybersecurity posture. In that regard, this Regulation should include the reporting of incidents that, on the basis of an initial assessment carried out by the Union entity concerned, could cause severe operational disruption to the functioning of, 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 network and information systems affected, 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.

(37) As the infrastructure and network and information systems 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. To that end, the Union entity affected should inform any relevant Member State counterparts designated or established pursuant to Articles 8 and 10 of Directive (EU) 2022/2555 of the occurrence of a significant incident about which it is reporting to CERT-EU. Where CERT-EU becomes aware of a significant incident occurring within a Member State, it should notify any relevant counterpart in that Member State.

(38) A mechanism to ensure effective exchange of information, coordination, and cooperation of the Union entities in the case of major incidents should be implemented, including a clear identification of the roles and responsibilities of the Union entities involved. The Commission representative in the IICB should, subject to 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 the European cyber crisis liaison organisation network (EU-CyCLONe), as a contribution to the shared situational awareness. The role of the Commission representative in the IICB as the point of contact should be without prejudice to the Commission's separate and distinct role in EU-CyCLONe pursuant to Article 16(2) of Directive (EU) 2022/2555.

(39) Regulation (EU) 2018/1725 of the European Parliament and of the Council[1] applies to any processing of personal data pursuant to 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 pursuant to this Regulation should comply 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 such compliance in an accountable manner.

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

---

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

(41) 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 Article 10(2), point (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 in 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.

(42) Pursuant to Article 33 of Regulation (EU) 2018/1725, Union entities and CERT-EU 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, the application of audit trail principles, the adoption of chain of custody, the storage of data at rest in a controlled and auditable environment, 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 a Union entity or CERT-EU transfers personal data related to an incident, including special categories of personal 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, the Union entities and CERT-EU should ensure that the third party applies measures concerning the protection of personal data at a level equivalent to Regulation (EU) 2018/1725.

(43) 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 set retention periods which are limited to what is necessary to achieve the specified purposes. In particular in relation to personal data collected for incident handling, Union entities and CERT-EU should differentiate between personal data that are collected for the detection of a cyber threat in their ICT environments to prevent an incident and personal data that are 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 personal data are necessary to trace and handle a recurrent incident or an incident of similar nature for which a correlation could be demonstrated.

(44) The handling of information by Union entities and CERT-EU should comply with the applicable rules on information security. The inclusion of human resources security as a cybersecurity risk-management measure should also comply with the applicable rules.

(45) For the purpose of sharing information, visible markings are used to indicate that sharing boundaries are to be applied by the recipients of information on the basis of, 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 CSIRTs and in some information analysis and sharing centres.

(46) This Regulation should be evaluated on a regular basis in light of future negotiations of multiannual financial 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.

(47) 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 the IICB, should evaluate the appropriateness of including network and information systems handling EUCI within the scope of this Regulation, in particular in the absence of information security rules common to Union entities.

(48) In accordance with the principle of proportionality, it is necessary and appropriate for the achievement of the basic objective of achieving a high common level of cybersecurity within Union entities to lay down rules on cybersecurity for Union entities. This Regulation does not go beyond what is necessary in order to achieve the objective pursued, in accordance with Article 5(4) of the Treaty on European Union.

(49) This Regulation reflects the fact that Union entities differ in size and capacity, including in terms of financial and human resources.

(50) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 and delivered an opinion on 17 May 2022[1],

HAVE ADOPTED THIS REGULATION:

[1] OJ C 258, 5.7.2022, p. 10.

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 pursuant to Article 6;

(b) cybersecurity risk management, reporting and information sharing;

(c) the organisation, functioning and operation of the Interinstitutional Cybersecurity Board established pursuant to Article 10, as well as the organisation, functioning and operation of the Cybersecurity Service for the Union institutions, bodies, offices and agencies (CERT-EU);

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

Article 2

Scope

1. This Regulation applies to Union entities, to the Interinstitutional Cybersecurity Board established pursuant to Article 10 and to CERT-EU.

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

3. With the exception of Article 13(8), this Regulation does not apply to network and information systems handling EU classified information (EUCI).

Article 3

Definitions

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

(1) ‘Union entities’ means the Union institutions, bodies, offices and agencies set up by or pursuant to the Treaty on European Union, the Treaty on the Functioning of European Union (TFEU) 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 body or coordination and oversight body that is responsible for the functioning of a Union entity, at the most senior administrative level, with a mandate to adopt or authorise decisions in line with the high-level governance arrangements of that Union entity, without prejudice to the formal responsibilities of other levels of management for compliance and cybersecurity risk management in their respective areas of responsibility;

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

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

(8) ‘major incident’ means an 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) ‘large-scale cybersecurity incident’ means a large-scale cybersecurity incident as defined in Article 6, point (7), of Directive (EU) 2022/2555;

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

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

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

(13) ‘vulnerability’ means a 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;

(15) ‘cloud computing service’ means a cloud computing service as defined in Article 6, point (30), of Directive (EU) 2022/2555.

Article 4

Processing of personal data

1. The processing of personal data under this Regulation by CERT-EU, the Interinstitutional Cybersecurity Board established pursuant to Article 10 and Union entities shall be carried out in accordance with Regulation (EU) 2018/1725.

2. Where they perform tasks or fulfil obligations pursuant to this Regulation, CERT-EU, the Interinstitutional Cybersecurity Board established pursuant to Article 10 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 to be necessary for reasons of substantial public interest pursuant to Article 10(2), point (g), of that Regulation. Such data may be processed only to the extent necessary for the implementation of cybersecurity risk-management measures referred to in Articles 6 and 8, for the provision of services by CERT-EU pursuant to Article 13, for the sharing of incident-specific information pursuant to Article 17(3) and Article 18(3), for the sharing of information pursuant Article 20, for the reporting obligations pursuant to Article 21, for incident response coordination and cooperation pursuant to Article 22 and for the management of major incidents pursuant to Article 23 of this Regulation. The Union entities and CERT-EU, when acting as data controllers, shall apply technical measures to prevent the processing of special categories of personal data for other purposes and shall 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 5

Implementation of measures

1. By … [eight months from the date of entry into force of this Regulation], the Interinstitutional Cybersecurity Board established pursuant to Article 10 shall, after consulting the European Union Agency for Cybersecurity (ENISA) and after receiving guidance from CERT-EU, issue guidelines to Union entities for the purpose of carrying out an initial cybersecurity review and establishing an internal cybersecurity risk-management, governance and control framework pursuant to Article 6, carrying out cybersecurity maturity assessments pursuant to Article 7, taking cybersecurity risk-management measures pursuant to Article 8, and adopting the cybersecurity plan pursuant to Article 9.

2. When implementing Articles 6 to 9, Union entities shall take into account the guidelines referred to in paragraph 1 of this Article, as well as relevant guidelines and recommendations adopted pursuant to Articles 11 and 14.

Article 6

Cybersecurity risk-management, governance and control framework

1. By … [15 months from the date of entry into force of this Regulation], each Union entity shall, after carrying out an initial cybersecurity review, such as an audit, establish an internal cybersecurity risk-management, governance and control framework (the 'Framework'). The establishment of the Framework shall be overseen by and under the responsibility of the Union entity's highest level of management.

2. The Framework shall cover the entirety of the unclassified ICT environment of the Union entity concerned, including any on-premises 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 those environments (ICT environment). The Framework shall be based on an all-hazards approach.

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

4. The Framework shall be reviewed on a regular basis, in light of the changing cybersecurity risks, and at least every four years. Where appropriate and following a request from the Interinstitutional Cybersecurity Board established pursuant to Article 10, a Union entity's Framework may be updated on the basis of guidance from CERT-EU on incidents identified or possible gaps observed in the implementation of this Regulation.

5. The highest level of management of each Union entity shall be responsible for the implementation of this Regulation and shall oversee the compliance of its organisation with the obligations related to the Framework.

6. 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 specific obligations under this Regulation to senior officials within the meaning of Article 29(2) of the Staff Regulations or other officials at equivalent level, within the Union entity concerned. Regardless of any such delegation, the highest level of management may be held liable for infringements of this Regulation by the Union entity concerned.

7. 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 establishing that percentage.

8. 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 report directly to the highest level of management on a regular basis on the state of the implementation. Without prejudice to the local cybersecurity officer being the single point of contact in each Union entity, a Union entity may delegate certain tasks of the local cybersecurity officer with regard 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 those tasks may be shared by several Union entities. Where those tasks are delegated to CERT-EU, the Interinstitutional Cybersecurity Board established pursuant to Article 10 shall decide whether the provision of that service is to be part of the baseline services of CERT-EU, taking into account the human and financial resources of the Union entity concerned. Each Union entity shall, without undue delay, notify CERT-EU of the local cybersecurity officer appointed and any subsequent change thereto.

CERT-EU shall establish and keep updated a list of appointed local cybersecurity officers.

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

Article 7

Cybersecurity maturity assessments

1. By … [18 months from the date of entry into force of this Regulation] and at least every two years thereafter, each Union entity shall carry out a cybersecurity maturity assessment incorporating all the elements of its ICT environment.

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 cybersecurity maturity assessments for their respective entities.

4. On the basis of a request of the Interinstitutional Cybersecurity Board established pursuant to Article 10 and with the explicit consent of the Union entity concerned, the results of a cybersecurity maturity assessment may be discussed within that Board or within the informal group of local cybersecurity officers with a view to learning from experience and sharing best practices.

Article 8

Cybersecurity risk-management measures

1. Without undue delay and in any event by … [20 months from the date of entry into force of this Regulation], each Union entity shall, under the oversight of its highest level of management, take appropriate and proportionate technical, operational and organisational measures to manage the cybersecurity 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 cybersecurity risks posed. When assessing the proportionality of those measures, due account shall be taken of the degree of the Union entity's exposure to cybersecurity risks, its size and the likelihood of occurrence of incidents and their severity, including their societal, economic and interinstitutional impact.

2. Union entities shall address at least the following domains in the implementation of the cybersecurity risk-management measures:

(a) cybersecurity policy, including measures needed to reach objectives and priorities referred to in Article 6 and paragraph 3 of this Article;

(b) policies on cybersecurity risk analysis and information system security;

(c) policy objectives regarding the use of cloud computing services;

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

(e) implementation of recommendations resulting from cybersecurity audits referred to in point (d) through cybersecurity and policy updates;

(f) organisation of cybersecurity, including establishment 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 and maintenance, including policies on vulnerability handling and disclosure;

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

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

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

(o) business continuity management, such as backup management and disaster recovery, and crisis management; and

(p) promotion and development of cybersecurity education, skills, awareness-raising, exercise and training programmes.

For the purposes of the first subparagraph, point (m), 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.

3. Union entities shall take 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 use 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) where appropriate, secured voice, video and text communications, and secured emergency communications systems within the Union entity;

(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;

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

(i) regular cybersecurity training of staff members;

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

(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) contractual obligations to report incidents, vulnerabilities and cyber threats as well as to have appropriate incident response and monitoring mechanisms in place.

Article 9

Cybersecurity plans

1. Following the conclusion of the cybersecurity maturity assessment carried out pursuant to Article 7 and taking into account the assets and cybersecurity risks identified in the Framework as well as the cybersecurity risk-management measures taken pursuant to Article 8, the highest level of management of each Union entity shall approve a cybersecurity plan without undue delay and in any event by … [24 months from the date of 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 include at least the cybersecurity risk-management measures taken pursuant to Article 8. The cybersecurity plan shall be revised every two years, or more frequently where necessary, following the cybersecurity maturity assessments carried out pursuant to Article 7 or any substantial review of the Framework.

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

3. The Union entity shall submit the completed cybersecurity plan to the Interinstitutional Cybersecurity Board established pursuant to Article 10.

Chapter III
Interinstitutional Cybersecurity Board

Article 10

Interinstitutional Cybersecurity Board

1. An Interinstitutional Cybersecurity Board (IICB) is hereby 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 Council of the European Union;

(iv) the Commission;

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

(vi) the European Central Bank;

(vii) the 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) ENISA;

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

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

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

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

4. Members of the IICB may be assisted by an alternate. Other representatives of the Union entities referred to in paragraph 3 or of other Union entities may be invited by the Chair to attend IICB meetings without voting power.

5. The Head of CERT-EU and the Chairs of the Cooperation Group, the CSIRTs network and EU-CyCLONe established, respectively, pursuant to Articles 14, 15 and 16 of Directive (EU) 2022/2555, or their alternates, may participate in IICB meetings as observers. In exceptional cases, the IICB may, in accordance with its internal rules of procedure, decide otherwise.

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

7. The IICB shall designate a Chair in accordance with its internal rules of procedure, from among its members for a period of three years. The Chair's alternate shall become a full member of the IICB for the same duration.

8. The IICB shall meet at least three times a year at the initiative of its Chair, at the request of CERT-EU or at the request of any of its members.

9. 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 of the IICB shall not have a vote except in the event of a tied vote, in which case the Chair may cast a deciding vote.

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

11. The secretariat of the IICB shall be provided by the Commission and shall be accountable to the Chair of the IICB.

12. The representatives nominated by the EUAN shall relay the IICB's decisions to the members of the EUAN. Any member of the 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.

14. By … [12 months from the date of entry into force of this Regulation] and on an annual basis thereafter, the IICB shall submit a report to the European Parliament and to the Council detailing progress made with the implementation of this Regulation and specifying in particular the extent of cooperation of CERT-EU with Member State counterparts in each of the Member States. The report shall constitute an input to the biennial report on the state of cybersecurity in the Union adopted pursuant to Article 18 of Directive (EU) 2022/2555.

Article 11

Tasks of the IICB

When exercising its responsibilities, the IICB shall, in particular:

(a) provide guidance to the Head of CERT-EU;

(b) effectively monitor and supervise the implementation of this Regulation and support the Union entities in strengthening their cybersecurity, including, where appropriate, requesting ad-hoc reports from Union entities and CERT-EU;

(c) following a strategic discussion, adopt a multiannual strategy on raising the level of cybersecurity in the Union entities, asses that strategy on a regular basis and in any event every five years and, where necessary, amend that strategy;

(d) establish the methodology and organisational aspects for the conduct 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, ensuring that such peer reviews are conducted by cybersecurity experts designated by a Union entity different from the Union entity being reviewed and that the methodology is based on Article 19 of Directive (EU) 2022/2555 and is, where appropriate, adapted to the Union entities;

(e) approve, on the basis of a proposal by the Head of CERT-EU, CERT-EU's annual work programme and monitor its implementation;

(f) approve, on the basis of a proposal by the Head of CERT-EU, CERT-EU's service catalogue and any updates thereof;

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

(h) approve, on the basis of a proposal by the Head of CERT-EU, the arrangements for service level agreements;

(i) 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;

(j) approve and monitor key performance indicators (KPIs) for CERT-EU established on the basis of a proposal by the Head of CERT-EU;

(k) approve cooperation arrangements, service level agreements or contracts between CERT-EU and other entities pursuant to Article 18;

(l) adopt guidelines and recommendations on the basis of a proposal by CERT-EU in accordance with Article 14 and instruct CERT-EU to issue, withdraw or modify a proposal for guidelines or recommendations, or a call for action;

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

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

(o) facilitate the establishment of an informal group of local cybersecurity officers of Union entities, supported by ENISA, with the aim of exchanging best practices and information in relation to the implementation of this Regulation;

(p) taking into account the information on the identified cybersecurity 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;

(q) establish a cyber crisis management plan with a view to supporting, at an operational level, the coordinated management of major incidents 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;

(r) coordinate the adoption of individual Union entities' cyber crisis management plans referred to in Article 9(2);

(s) adopt recommendations relating to supply chain security referred to in Article 8(2), first subparagraph, 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 12

Compliance

1. The IICB shall, pursuant to Article 10(2) and Article 11, effectively monitor the implementation of this Regulation and of adopted guidelines, 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 Union entity concerned is directly represented on the IICB, that Union entity shall not have voting rights.

2. Where the IICB finds that a Union entity has not effectively implemented this Regulation or guidelines, recommendations or calls for action issued pursuant thereto, it may, without prejudice to the internal procedures of the Union entity concerned, and after giving an 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, guidelines to the Union entity concerned to ensure that its Framework, cybersecurity risk-management measures, cybersecurity plan and reporting comply 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 concerned pursuant to this Regulation;

(d) issue a reasoned notification to the Union entity concerned, in the event 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, inform the Court of Auditors, within the remit of its mandate, of the alleged non-compliance;

(g) issue a recommendation that all Member States and Union entities implement a temporary suspension of data flows to the Union entity concerned.

For the purposes of the first subparagraph, point (c), the audience of a warning shall be restricted appropriately, where necessary in view of the cybersecurity risk.

Warnings and recommendations issued pursuant to the first subparagraph shall be directed to the highest level of management of the Union entity concerned.

3. Where the IICB has adopted measures under paragraph 2, first subparagraph, points (a) to (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.

4. Where the IICB considers that there is persistent infringement of this Regulation by a Union entity resulting directly from actions or omissions of an official or other servant of the Union, including at the highest level of management, the IICB shall request that the Union entity concerned take appropriate action, including requesting it to consider taking action of a disciplinary nature, in accordance with the rules and procedures laid down in the Staff Regulations and any other applicable rules and procedures. To that end, the IICB shall transfer the necessary information to the Union entity concerned.

5. Where Union entities notify that they are unable to meet the deadlines set out in Article 6(1) and Article 8(1), the IICB may, in duly substantiated cases, taking into account the size of the Union entity, authorise the extension of those deadlines.

Chapter IV
CERT-EU

Article 13

CERT-EU mission and tasks

1. CERT-EU's mission shall be to contribute to the security of the unclassified ICT environment of 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.

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

3. CERT-EU shall carry out the following tasks to assist the Union entities:

   (a) support them with the implementation of this Regulation and contribute to the coordination of the implementation of this Regulation through the measures listed in Article 14(1) or through ad-hoc reports requested by the IICB;

(b) offer standard CSIRT services for Union entities by means of 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 17 and 18;

(d) bring to the attention of the IICB any problems relating to the implementation of this Regulation and the implementation of guidelines, recommendations and calls for action;

(e) on the basis of the information referred to in paragraph 2, contribute to the Union cyber situational awareness in close cooperation with ENISA;

(f) coordinate the management of major incidents;

(g) act on the part of Union entities as the equivalent of the coordinator designated for the purposes of coordinated vulnerability disclosure pursuant to Article 12(1) of Directive (EU) 2022/2555;

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

The information referred to in the first subparagraph, point (e), shall be shared with the IICB, the CSIRTs network and the European Union Intelligence and Situation Centre (EU INTCEN), where applicable and appropriate, and subject to appropriate confidentiality conditions.

4. CERT-EU may, in accordance with Article 17 or 18 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 CSIRTs network, including with regard to mutual assistance;

(c) cyber threat intelligence, including situational awareness;

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

5. Within its competence, 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.

6. 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 3, on the basis of service level agreements and subject to available resources, in particular broad-spectrum network monitoring, including first-line 24/7 monitoring for high-severity cyber 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;

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

(d) 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 tasks or responsibilities conferred under Union law, on the basis of written agreements and with the prior approval of the IICB.

With regard to the first subparagraph, point (d), CERT-EU may, on an exceptional basis, enter into service level agreements with entities other than the Union entities with the prior approval of the IICB.

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

8. CERT-EU may provide assistance to Union entities regarding incidents in network and information systems handling EUCI where 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.

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

10. 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 major incidents and the manner in which they were handled. That information shall be included in the report referred to in Article 10(14).

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

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

Article 14

Guidelines, recommendations and calls for action

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

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

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

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

With regard to the first subparagraph, point (a), the Union entity concerned shall, without undue delay after receiving the call for action, inform CERT-EU of how the urgent security measures were applied.

2. Guidelines and recommendations may include:

(a) common methodologies and a model for assessing the cybersecurity maturity of the Union entities, including the corresponding scales or KPIs, 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;

(b) arrangements for or improvements to cybersecurity risk management and the cybersecurity risk-management measures;

(c) arrangements for cybersecurity maturity assessments and cybersecurity plans;

(d) 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;

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

(f) information-sharing arrangements pursuant to Article 20.

Article 15

Head of CERT-EU

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

2. The Head of CERT-EU shall be responsible for the proper functioning of CERT-EU and shall act within the remit of his or her role and under the direction of the IICB. The Head of CERT-EU shall report regularly to the Chair of the IICB and shall 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 Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council[1], and shall report regularly to the authorising officer by delegation on the implementation of measures in respect of which powers have been sub-delegated to the Head of CERT-EU.

4. The Head of CERT-EU shall draw up, on an annual basis, a financial planning of administrative revenue and expenditure for its activities, a proposed annual work programme, a proposed service catalogue for CERT-EU, proposed revisions of the service catalogue, proposed arrangements for service level agreements and proposed KPIs for CERT-EU, to be approved by the IICB in accordance with Article 11. 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.

---

1 Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union, amending Regulations (EU) No 1296/2013, (EU) No 1301/2013, (EU) No 1303/2013, (EU) No 1304/2013, (EU) No 1309/2013, (EU) No 1316/2013, (EU) No 223/2014, (EU) No 283/2014, and Decision No 541/2014/EU and repealing Regulation (EU, Euratom) No 966/2012 (OJ L 193, 30.7.2018, p. 1).

5. The Head of CERT-EU shall submit reports at least annually to the IICB and the Chair of the IICB 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 11. Those reports shall include a work programme for the following 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 with regard to financial and human resources.

Article 16

Financial and staffing matters

1. CERT-EU shall be integrated into the administrative structure of a directorate-general of the Commission in order to benefit from the Commission's administrative, financial management and accounting support structures, while maintaining its status as an autonomous interinstitutional service provider for all Union entities. The Commission shall inform the IICB of the administrative location of CERT-EU and any changes thereto. The Commission shall review the administrative arrangements related to CERT-EU on a regular basis and in any event before the establishment of any multiannual financial framework pursuant to Article 312 TFEU, in order to allow for appropriate action to be taken. The review shall include the possibility of establishing 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 and under the supervision of the IICB.

3. CERT-EU's tasks and activities, including services provided by CERT-EU pursuant to Article 13(3), (4), (5) and (7) and Article 14(1) to Union entities financed from the heading of the multiannual financial framework dedicated to European public administration, shall be funded by means of a distinct budget line of the Commission budget. The posts earmarked for CERT-EU shall be detailed in a footnote to the Commission establishment plan.

4. Union entities other than those referred to in paragraph 3 of this Article shall make an annual financial contribution to CERT-EU to cover the services provided by CERT-EU pursuant to that paragraph. The contributions shall be based on orientations given by the IICB and agreed between each Union 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 of this Article, as internal assigned revenue, as provided for in Article 21(3), point (c), of Regulation (EU, Euratom) 2018/1046.

5. The costs of the services provided for in Article 13(6) shall be recovered from the Union entities receiving CERT-EU services. The revenues shall be assigned to the budget lines supporting the costs.

Article 17

Cooperation of CERT-EU with Member State counterparts

1. CERT-EU shall, without undue delay, cooperate and exchange information with Member State counterparts, in particular the CSIRTs designated or established pursuant to Article 10 of Directive (EU) 2022/2555, or, where applicable, the competent authorities and single points of contact designated or established pursuant to Article 8 of that Directive, with regard to incidents, cyber threats, vulnerabilities, 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 by means of the CSIRTs network established pursuant to Article 15 of Directive (EU) 2022/2555. CERT-EU shall support the Commission in EU-CyCLONe established pursuant to Article 16 of Directive (EU) 2022/2555 on the coordinated management of large-scale cybersecurity incidents and crises.

2. Where CERT-EU becomes aware of a significant incident occurring within the territory of a Member State, it shall, without delay, notify any relevant counterpart in that Member State, in accordance with paragraph 1.

3. Provided that personal data are protected in accordance with applicable Union data protection law, CERT-EU shall, without undue delay, exchange relevant incident-specific information with Member State counterparts 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 exchange incident-specific information which reveals the identity of the target of the incident only in the event of one of the following:

(a) the Union entity affected consents;

(b) the Union entity affected does not consent as provided for in point (a) but the disclosure of the identity of the Union entity affected would increase the probability that incidents elsewhere would be avoided or mitigated;

(c) the Union entity affected has already made public that it was affected.

Decisions to exchange incident-specific information which reveals the identity of the target of the incident pursuant to the first subparagraph, point (b), shall be endorsed by the Head of CERT-EU. Prior to issuing such a decision, CERT-EU shall contact the Union entity affected in writing, explaining clearly how the disclosure of its identity would help to avoid or mitigate incidents elsewhere. The Head of CERT-EU shall provide the explanation and explicitly request the Union entity to state whether it consents within a set timeframe. The Head of CERT-EU shall also inform the Union entity that, in light of the explanation provided, he or she reserves the right to disclose the information even in the absence of consent. The Union entity affected shall be informed before the information is disclosed.

Article 18

Cooperation of CERT-EU with other counterparts

1. CERT-EU may cooperate with counterparts in the Union other than those referred to in Article 17 which 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. Where CERT-EU establishes cooperation with such counterparts, it shall inform any relevant Member State counterparts referred to in Article 17(1), in the Member State in which the counterpart is located. Where applicable and appropriate, such cooperation and the conditions thereof, including regarding cybersecurity, data protection and information handling, shall be established 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 the case of an urgent and imminent need to exchange cybersecurity information in the interests of Union 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 CERT-EU does not have a confidentiality arrangement in place with that entity. In such cases, CERT-EU shall immediately inform the Chair of the IICB, and shall report to the IICB by means of regular reports or meetings.

2. CERT-EU may cooperate with partners, such as commercial entities, including industry sector-specific entities, international organisations, non-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, with the consent of the Union entity affected by an incident and provided that a non-disclosure arrangement or contract is in place with the relevant counterpart or partner, provide information related to the specific incident to counterparts or partners referred to in paragraphs 1 and 2 solely for the purpose of contributing to its analysis.

Chapter V
Cooperation and reporting obligations

Article 19

Information handling

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

2. Regulation (EC) No 1049/2001 of the European Parliament and of the Council[1] shall apply with regard to requests for public access to documents held by CERT-EU, including the obligation under that Regulation to consult other Union entities or, where relevant, Member States, whenever a request concerns their documents.

3. The handling of information by Union entities and CERT-EU shall comply with the applicable rules on information security.

Article 20

Cybersecurity information-sharing arrangements

1. Union entities may, on a voluntary basis, notify CERT-EU of, and provide it with information on, incidents, cyber threats, 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 Article 12, 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] 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).

2. To perform its mission and tasks conferred pursuant to Article 13, 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 incidents. The requested Union entity shall transmit the requested information, and any subsequent updates thereto, without undue delay.

3. CERT-EU may exchange incident-specific information with Union entities which reveals the identity of the Union entity affected by the incident, provided that the Union entity affected consents. Where a Union entity withholds its consent, it shall provide CERT-EU with reasons substantiating that decision.

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

5. The IICB or CERT-EU, as applicable, shall, upon request, share guidelines, recommendations and calls for action with the European Parliament and the Council.

6. The sharing obligations laid down in this Article 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

Reporting obligations

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

(a) it has caused or is capable of causing severe operational disruption to the functioning of, or financial loss to, the Union entity concerned;

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

2. 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 that the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-entity or a cross-border impact;

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

(i) a 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 incident;

(e) in the event of an ongoing incident 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 of their handling of the incident.

3. A Union entity shall, without undue delay and in any event within 24 hours of becoming aware of a significant incident, inform any relevant Member State counterparts referred to in Article 17(1) in the Member State where it is located that a significant incident has occurred.

4. The Union entities shall notify, inter alia, any information enabling CERT-EU to determine any cross-entity impact, impact on the hosting Member State or cross-border impact following a significant incident. Without prejudice to Article 12, the mere act of notification shall not subject the Union entity to increased liability.

5. Where applicable, Union entities shall communicate, without undue delay, to the users of the network and information systems affected, or of 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, any measures or remedies that they can take in response to that incident or that threat. Where appropriate, Union entities shall inform those users of the significant cyber threat itself.

6. 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.

7. 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 provide further details of the types of information that it requires for situational awareness and incident response.

8. CERT-EU shall submit to the IICB, ENISA, the EU INTCEN and the CSIRTs network, every three months, a summary report including anonymised and aggregated data on significant incidents, incidents, cyber threats, near misses and vulnerabilities pursuant to Article 20 and significant incidents notified pursuant to paragraph 2 of this Article. The summary report shall constitute an input to the biennial report on the state of cybersecurity in the Union adopted pursuant to Article 18 of Directive (EU) 2022/2555.

9. By … [6 months from the date of entry into force of this Regulation], the IICB shall issue guidelines or recommendations further specifying the arrangements for, and format and content of, the reporting pursuant to this Article. When preparing such guidelines or recommendations, the IICB shall take into account any implementing acts adopted pursuant to Article 23(11) of Directive (EU) 2022/2555 specifying the type of information, the format and the procedure of notifications. CERT-EU shall disseminate the appropriate technical details to enable proactive detection, incident response or mitigating measures by Union entities.

10. The reporting obligations laid down in this Article 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 22

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 incidents, cyber threats, vulnerabilities and near misses among:

(a) Union entities;

(b) the counterparts referred to in Articles 17 and 18.

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 relevant to Union entities, or providing assistance, where 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 incidents, cyber threats, vulnerabilities and near misses as well as sharing relevant developments in the field of cybersecurity.

4. By … [12 months from the date of entry into force of this Regulation], the IICB shall, on the basis of a proposal by CERT-EU, adopt guidelines 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.

5. Following a specific request from a Member State and with the approval of the Union entities concerned, CERT-EU may call on experts from the list referred to in Article 23(4), for contributing to the response to a major incident which has an impact in that Member State, or a large-scale cybersecurity incident in accordance with Article 15(3), point (g), of Directive (EU) 2022/2555. Specific rules on access to and the use of technical experts from Union entities shall be approved by the IICB on the basis of a proposal by CERT-EU.

Article 23

Management of major incidents

1. In order to support at operational level the coordinated management of major incidents 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 11, point (q), establish a cyber crisis management plan based on the activities referred to in Article 22(2), in close cooperation with CERT-EU and ENISA. The cyber crisis management plan shall include at least the following elements:

   (a) arrangements concerning coordination and information flow 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 that are to be used.

2. The Commission representative in the IICB shall, subject to the cyber crisis management plan established pursuant to paragraph 1 of this Article 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.

3. CERT-EU shall coordinate among the Union entities the management of major incidents. It shall maintain an inventory of the available technical expertise that would be needed for incident response in the event of major incidents and assist the IICB in coordinating Union entities' cyber crisis management plans for major incidents referred to in Article 9(2).

4. 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 24

Initial budgetary reallocation

In order to ensure the 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 Union annual budget adopted following the entry into force of this Regulation.

Article 25

Review

1. By … [12 months from the date of entry into force of this Regulation] and on an annual basis thereafter, the IICB, with the assistance of CERT-EU, shall report to the Commission on the implementation of this Regulation. The IICB may make recommendations to the Commission to review this Regulation.

2. By … [36 months from the date of entry into force of this Regulation] and every two years thereafter, 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 to the Council.

The report referred to in the first subparagraph of this paragraph shall include the review referred to in Article 16(1), on the possibility of establishing CERT-EU as a Union office.

3. By … [five years from the date of entry into force of this Regulation], the Commission shall evaluate the functioning of this Regulation and submit a report to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. The Commission shall also evaluate the appropriateness of including network and information systems handling 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 26

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 Strasbourg,

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