EUROPEAN
COMMISSION

Brussels, 22.3.2022
COM(2022) 122 final

2022/0085 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

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

{SWD(2022) 67 final} - {SWD(2022) 68 final}

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

• Reasons for and objectives of the proposal

This proposal establishes a framework for ensuring common cybersecurity rules and measures among the Union institutions, bodies and agencies. It aims at further improving all entities' resilience and incident response capacities. It is in line with the Commission's priorities to make Europe fit for the digital age and to build a future-ready economy that works for the people. Moreover, ensuring a secure and resilient public administration is a cornerstone in the digital transformation of society as a whole.

This proposal builds on the EU Security Union Strategy (COM(2020) 605 final) and the EU's Cybersecurity Strategy for the Digital Decade (JOIN(2020) 18 final).

The proposal modernises the existing CERT-EU legal framework and takes account of the changed and increased digitisation of the institutions, bodies and agencies in recent years as well as the evolving cybersecurity threat landscape. Both developments have been further amplified since the onset of the COVID-19 crisis, while the number of incidents continues to rise, with increasingly sophisticated attacks coming from a wide range of sources.

The proposal renames CERT-EU from 'Computer Emergency Response Team' to 'Cybersecurity Centre' for the Union institutions, bodies and agencies, in line with developments in the Member States and globally, where many CERTs are renamed as Cybersecurity Centres, but keeps the short name 'CERT-EU' because of name recognition.

• Consistency with existing policy provisions in the policy area

This proposal is aimed at increasing the cybersecurity resilience of the Union institutions, bodies and agencies against cyber threats, while aligning with existing legislation:

- Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union. It also aligns with the proposal for a Directive (EU) XXXX/XXXX on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 [proposal NIS 2].
- Regulation (EU) 2019/881 on the European Union Agency for Cybersecurity and on information and communications technology cybersecurity certification (Cybersecurity Act).
- Proposal for a Regulation (EU) XXXX/XXXX on information security in the institutions, bodies, offices and agencies of the Union.
- Commission Recommendation of 23 June 2021 on building a Joint Cyber Unit.
- Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises.

The Annex to Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises sets out the Blueprint for coordinated response to large-scale cross-border cybersecurity incidents and crises.

In its resolution from 9 March 2021, the Council of the European Union stressed that cybersecurity is vital for the functioning of public administration at both national and EU level as well as for society and economy as a whole, underlining the importance of a robust and consistent security framework to protect all EU personnel, data, communication

networks, information systems and decision-making processes. In particular, this is to be achieved through enhanced resilience and improved security culture of the Union institutions, bodies and agencies. Sufficient resources and capabilities are to be made available, including in the context of the reinforcement of the mandate of CERT-EU.

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

• Legal basis

The legal basis for this Regulation is Article 298 of the Treaty on the Functioning of the European Union (TFEU) which provides that in carrying out their missions, the institutions, bodies, offices and agencies of the Union shall have the support of an open, efficient and independent European administration. In compliance with the Staff Regulations and the Conditions of Employment adopted on the basis of Article 336, the European Parliament and the Council, acting by means of regulations in accordance with the ordinary legislative procedure, shall establish provisions to that end.

Information technology has provided new ways for Union institutions, bodies and agencies to work, interact with citizens and improve overall operations. As technology continues to evolve, the cyber threat landscape evolves along with it. Union institutions, bodies and agencies have become highly attractive targets of sophisticated cyberattacks. The establishment of systems and requirements to ensure cybersecurity appears to be contributing to the efficiency and the independence of the European administration, so that Union institutions, bodies, offices and agencies can operate in a more efficient manner in a digital world in the conduct of their missions.

Moreover, current disparities, as explained in section 3 below, among Union institutions, bodies and agencies' cybersecurity posture and approach in the area of cybersecurity are further obstacles to an open, efficient and independent European administration. Without a common approach, the cybersecurity posture among Union institutions, bodies and agencies would continue to develop in divergent directions. This legal basis is therefore appropriate given that the Regulation aims to create a common legal framework for cybersecurity within Union institutions, bodies, offices and agencies.

• Subsidiarity

The Regulation laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union is within the remits of the Union's exclusive competence.

• Proportionality

The rules proposed in this Regulation do not go beyond what is necessary to meet the specific objectives satisfactorily. The envisaged measures will contribute to achieving a high common level of cybersecurity without exceeding what is necessary to achieve the objective in light of the increasingly high risks they face.

• Choice of the instrument

The choice of a Regulation, which is directly applicable, is considered the appropriate legal instrument to define and streamline the obligations imposed on Union institutions, bodies and agencies. In order to allow for targeted improvements, a regulation is the most appropriate legal instrument.

3. RESULTS OF EX-ANTE EVALUATIONS, STAKEHOLDER CONSULTATIONS AND IMPACT ASSESSMENTS

- **Ex-ante evaluations**

CERT-EU has conducted an assessment of the principal cyber threats to which Union institutions, bodies and agencies are currently exposed or are likely to be exposed to in the foreseeable future.

Three categories of observations were used in the analysis:

- Attempts to breach Union institutions, bodies and agencies' IT infrastructure (when successful, they are treated as incidents, in the other cases they are still recorded as detected attempts).
- Threats detected in the proximity of Union institutions, bodies and agencies (e.g. in their related sectors, their stakeholder communities or in Europe).
- Major threat trends observed globally.

Furthermore, the analysis considered how major ongoing shifts are affecting the ways in which Union institutions manage and use their IT infrastructure and services. Such shifts include:

- Increased teleworking.
- Migration of systems to the cloud.
- Increased outsourcing of IT services.

From 2019 to 2021, the number of significant incidents[1] affecting Union institutions, bodies and agencies, authored by advanced persistent threat (APT) actors, has surged dramatically. The first half of 2021 saw the equivalent in significant incidents as in the whole of 2020. This is also reflected in the number of forensics images (snapshots of the contents of affected systems or devices) CERT-EU analysed in 2020, which tripled in comparison to 2019, while the number of significant incidents rose more than ten-fold since 2018.

In 2020, CERT-EU's Steering Board set a new strategic aim for CERT-EU to guarantee a comprehensive level of cyber defence for all institutions, bodies and agencies with suitable breadth and depth and continuous adaptation to current or impending threats, including attacks against mobile devices, cloud environments and internet-of-things devices.

Complementary to the CERT-EU threat analysis, the Commission has carried out an evaluation of the cybersecurity functioning of 20 Union institutions, bodies and agencies. This provided insight into established cybersecurity practices, and cybersecurity management capabilities with external benchmarking of some technical security controls.

This evaluation was based on questionnaires to which these institutions, bodies and agencies responded, publicly available data, and data provided directly by the Union institutions, bodies and agencies themselves. It provides sufficient insights in the current situation to conclude:

- Cybersecurity maturity, IT infrastructure size and levels of capability vary substantially among the evaluated Union institutions, bodies and agencies.

[1] 'Significant incident' means any incident unless it has limited impact and is likely to be already well understood in terms of method or technology.

- Whereas there are mature detection and response capabilities among many Union institutions, bodies and agencies in general, there are varying levels of integrated risk management in their cybersecurity governance capabilities.
- Whereas in general cybersecurity frameworks (strategy, policy and a base of rules) of the evaluated Union institutions, bodies and agencies are well established in the key cybersecurity domains, listed in the Annex I of the Regulation, some Union institutions, bodies and agencies lack mature business continuity management, compliance, audit and continuous improvement.
- Technical measures considered best practices were found to be unevenly applied by the evaluated Union institutions, bodies and agencies.

In summary, the analysis of the 20 Union institutions, bodies and agencies shows that their governance, cyber-hygiene, overall capability and maturity vary over a broad spectrum. Therefore, requiring all Union institutions, bodies and agencies to implement a baseline of cybersecurity measures is instrumental to address this disparity in maturity and to bring all Union institutions, bodies and agencies to a high common level of cybersecurity.

No Union legislation has so far focussed on the cybersecurity of Union institutions, bodies and agencies and has comprehensively tackled the cybersecurity threat landscape and the emerging IT risks driven by digitalisation.

- **Stakeholder consultations**

The Commission has consulted stakeholders throughout the Union institutions, bodies and agencies as well as representatives of Member States in the Council and stakeholders in the European Parliament. On 25 June 2021, representatives of Member States and relevant stakeholders from the Union institutions, bodies and agencies participated in a workshop organised by the Commission to discuss the content of the future proposal for Regulation.

- **Impact assessment**

The impact of the present proposal will fall on Union institutions, bodies and agencies. This renders a specific impact assessment not necessary as it will not apply to Member States.

- **Fundamental rights**

The European Union is committed to ensuring high standards of protection of fundamental rights. All information sharing based on this Regulation would be conducted in trusted environments in full respect of the right to the protection of personal data as laid down in Article 8 of the Charter of Fundamental Rights of the European Union and the relevant data protection legislation, notably Regulation (EU) 2018/1725 of the European Parliament and of the Council.

4. BUDGETARY IMPLICATIONS

Market benchmarks and studies[2] show that direct cybersecurity spending has tended to vary between 4 and 7% of the aggregated IT expenditures of organisations. However, the threat analysis undertaken by CERT-EU in support of this legislative proposal indicates that

[2] Source: Gartner, 'Identifying the Real Information Security Budget' (2016). This is in addition to indirect spending IT security such as on network security such as firewalls, antivirus and system owner responsibilities such as risk assessment and the implementation of security controls. A 2020 paper puts cybersecurity spending at financial institutions at 10-11% of IT spending, source: DI_2020-FS-ISAC-Cybersecurity.pdf (deloitte.com).

international bodies and political organisations face increased risks and therefore a level of 10% of IT spending on cybersecurity would seem a more adequate target. The exact cost of such efforts cannot be determined due to the lack of detailed information on IT expenditure of the Union institutions, bodies and agencies and the relevant share of cybersecurity spending.

While it is therefore likely that many Union institutions, bodies and agencies spend less on cybersecurity than they should, this Regulation will not cause as such an increase in that current expenditure. Even without the Regulation each entity would need to ensure an adequate level of cybersecurity. The Regulation continues the previous cooperation in the Steering Board of CERT-EU and formalises a layer of information exchange already partly existing today. As detailed in the legislative financial statement, CERT-EU will require additional resources to fulfil its expanded role and these resources should be reallocated from the Union institutions, bodies and agencies benefitting from CERT-EU's services.

5. OTHER ELEMENTS

- **Implementation, monitoring, evaluation and reporting arrangements**

The Interinstitutional Cybersecurity Board (IICB), with the assistance of CERT-EU, should review the functioning of this Regulation, carry out evaluations, and present a report with its findings to the Commission. The Commission should ensure regular reporting to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions.

CERT-EU can draft a proposal for a guidance document or a recommendation, which the IICB can choose to adopt. A guidance document is an advisory directed towards all or a subset of the Union institutions, bodies and agencies whereas a recommendation is directed towards individual Union institutions, bodies and agencies. A call for action is a CERT-EU advisory describing urgent security measures which Union institutions, bodies and agencies are urged to take within a set timeframe.

- **Detailed explanation of the specific provisions of the proposal**

General provisions

The Regulation lays down measures with a view to ensuring a high common level of cybersecurity and it applies to the Union institutions, bodies and agencies to enable them to carry out their respective missions in an open, efficient and independent way. (Articles 1-3, 23-25)

Measures for a high common level of cybersecurity

Union institutions, bodies and agencies are obliged to establish an internal cybersecurity risk management, governance and control framework that ensures an effective and prudent management of all cybersecurity risks. The institutions, bodies and agencies shall moreover adopt a cybersecurity baseline to address the risks identified under the framework, carry out regular cybersecurity maturity assessments and adopt a cybersecurity plan. (Articles 4-8)

Interinstitutional Cybersecurity Board

The Interinstitutional Cybersecurity Board is established and shall be responsible for monitoring the implementation of this Regulation by the Union institutions, bodies and agencies as well as supervising the implementation of general priorities and objectives by CERT-EU and providing strategic direction to CERT-EU. (Articles 9-11).

CERT-EU

CERT-EU shall contribute to the security of the IT environment of all Union institutions, bodies and agencies by advising them, by helping to prevent, detect, mitigate and respond to incidents and by acting as their cybersecurity information exchange and incident response coordination hub. (Articles 12-17)

Cooperation and reporting obligations

The Regulation ensures cooperation and the exchange of information among CERT-EU, and the Union institutions, bodies and agencies to develop trust and confidence. To this end CERT-EU may request Union institutions, bodies and agencies to provide it with relevant information and CERT-EU may exchange incident-specific information with Union institutions, bodies and agencies to facilitate detection of similar cyber threats or incidents without the consent of the affected constituent. CERT-EU may only exchange incident-specific information which reveals the identity of the target of the cybersecurity incident with the consent of the affected constituent.

Notably, all Union institutions, bodies and agencies shall notify CERT-EU of significant cyber threats, significant vulnerabilities and significant incidents without undue delay and in any event no later than 24 hours after becoming aware of them. (Articles 18-22)

2022/0085 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

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

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

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

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

Having regard to the proposal from the European Commission,

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

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) In the digital age, information and communication technology is a cornerstone in an open, efficient and independent Union administration. Evolving technology and increased complexity and interconnectedness of digital systems amplify cybersecurity risks making the Union administration more vulnerable to cyber threats and incidents, which ultimately poses threats to the administration's business continuity and capacity to secure its data. While increased use of cloud services, ubiquitous use of IT, high digitalisation, remote work and evolving technology and connectivity are nowadays core features of all activities of the Union administration entities, digital resilience is not yet sufficiently built in.

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

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

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

(5) The Directive [proposal NIS 2] on measures for a high common level of cybersecurity across the Union aims to further improve the cybersecurity resilience and incident response capacities of public and private entities, national competent authorities and bodies as well as the Union as a whole. It is therefore necessary that Union institutions, bodies and agencies follow suit by ensuring rules that are consistent with the Directive [proposal NIS 2] and mirror its level of ambition.

(6) To reach a high common level of cybersecurity, it is necessary that each Union institution, body and agency establishes an internal cybersecurity risk management, governance and control framework that ensures an effective and prudent management of all cybersecurity risks, and takes account of business continuity and crisis management.

(7) The differences between Union institutions, bodies and agencies require flexibility in the implementation since one size will not fit all. The measures for a high common level of cybersecurity should not include any obligations directly interfering with the exercise of the missions of Union institutions, bodies and agencies or encroaching on their institutional autonomy. Thus, those institutions, bodies and agencies should establish their own frameworks for cybersecurity risk management, governance and control, and adopt their own baselines and cybersecurity plans.

(8) In order to avoid imposing a disproportionate financial and administrative burden on Union institutions, bodies and agencies, the cybersecurity risk management requirements should be proportionate to the risk presented by the network and information system concerned, taking into account the state of the art of such measures. Each Union institution, body and agency should aim to allocate an adequate percentage of its IT budget to improve its level of cybersecurity; in the longer term a target in the order of 10% should be pursued.

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

(10) Union institutions, bodies and agencies should assess risks related to relationships with suppliers and service providers, including providers of data storage and processing services or managed security services, and take appropriate measures to address them. These measures should form part of the cybersecurity baseline and be further specified in guidance documents or recommendations issued by CERT-EU. When defining measures and guidelines, due account should be taken of relevant EU legislation and policies, including risk assessments and recommendations issued by the NIS Cooperation Group, such as the EU Coordinated risk assessment and EU Toolbox on

5G cybersecurity. In addition, certification of relevant ICT products, services and processes could be required, under specific EU cybersecurity certification schemes adopted pursuant to Article 49 of Regulation EU 2019/881.

(11) In May 2011, the Secretaries-General of the Union institutions and bodies decided to establish a pre-configuration team for a computer emergency response team for the Union's institutions, bodies and agencies (CERT-EU) supervised by an inter-institutional Steering Board. In July 2012, the Secretaries-General confirmed the practical arrangements and agreed to maintain CERT-EU as a permanent entity to continue to help improve the overall level of information technology security of the Union's institutions, bodies and agencies as an example of visible inter-institutional cooperation in cybersecurity. In September 2012, CERT-EU was established as a Taskforce of the European Commission with an interinstitutional mandate. In December 2017, the Union institutions and bodies concluded an interinstitutional arrangement on the organisation and operation of CERT-EU[3]. This arrangement should continue to evolve to support the implementation of this Regulation.

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

(13) Many cyberattacks are part of wider campaigns that target groups of Union institutions, bodies and agencies or communities of interest that include Union institutions, bodies and agencies. To enable proactive detection, incident response or mitigating measures, Union institutions, bodies and agencies should notify CERT-EU of significant cyber threats, significant vulnerabilities and significant incidents and share appropriate technical details that enable detection or mitigation of, as well as response to, similar cyber threats, vulnerabilities and incidents in other Union institutions, bodies and agencies. Following the same approach as the one envisaged in Directive [proposal NIS 2], where entities become aware of a significant incident they should be required to submit an initial notification to CERT-EU within 24 hours. Such information exchange should enable CERT-EU to disseminate the information to other Union institutions, bodies and agencies, as well as to appropriate counterparts, to help protect the Union IT environments and the Union's counterparts' IT environments against similar incidents, threats and vulnerabilities.

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

(15) CERT-EU should support the implementation of measures for a high common level of cybersecurity through proposals for guidance documents and recommendations to the IICB or by issuing calls for action. Such guidance documents and recommendations should be approved by the IICB. When needed, CERT-EU should issue calls for

[3] OJ C 12, 13.1.2018, p. 1–11.

action describing urgent security measures which Union institutions, bodies and agencies are urged to take within a set timeframe.

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

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

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

(19) CERT-EU should also fulfil the role provided for it in Directive [proposal NIS 2] concerning cooperation and information exchange with the computer security incident response teams (CSIRTs) network. Moreover, in line with Commission Recommendation (EU) 2017/1584[4], CERT-EU should cooperate and coordinate on the response with the relevant stakeholders. In order to contribute to a high level of cybersecurity across the Union, CERT-EU should share incident specific information with national counterparts. CERT-EU should also collaborate with other public as well as private counterparts, including at NATO, subject to prior approval by the IICB.

(20) In supporting operational cybersecurity, CERT-EU should make use of the available expertise of the European Union Agency for Cybersecurity through structured cooperation as provided for in Regulation (EU) 2019/881 of the European Parliament and of the Council[5]. Where appropriate, dedicated arrangements between the two entities should be established to define the practical implementation of such cooperation and to avoid the duplication of activities. CERT-EU should cooperate with the European Union Agency for Cybersecurity on threat analysis and share its threat landscape report with the Agency on a regular basis.

---

4 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).

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

(21) In support of the Joint Cyber Unit built in accordance with the Commission Recommendation of 23 June 2021[6], CERT-EU should cooperate and exchange information with stakeholders to foster operational cooperation and to enable the existing networks in realising their full potential in protecting the Union.

(22) All personal data processed under this Regulation should be processed in accordance with data protection legislation including Regulation (EU) 2018/1725 of the European Parliament and of the Council.[7]

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

(24) As the services and tasks of CERT-EU are in the interest of all Union institutions, bodies and agencies, each Union institution, body and agency with IT expenditure should contribute a fair share to those services and tasks. Those contributions are without prejudice to the budgetary autonomy of the Union institutions, bodies and agencies.

(25) The IICB, with the assistance of CERT-EU, should review and evaluate the implementation of this Regulation and should report its findings to the Commission. Building on this input, the Commission should report to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions.

HAVE ADOPTED THIS REGULATION:

Chapter I
GENERAL PROVISIONS

Article 1
Subject-matter

This Regulation lays down:

(a) obligations on Union institutions, bodies and agencies to establish an internal cybersecurity risk management, governance and control framework;

(b) cybersecurity risk management and reporting obligations for Union institutions, bodies and agencies;

(c) rules on the organisation and operation of the Cybersecurity Centre for the Union institutions, bodies and agencies (CERT-EU) and on the organisation and operation of the Interinstitutional Cybersecurity Board.

---

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

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

Article 2
Scope

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

Article 3
Definitions

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

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

(2) 'network and information system' means network and information system within the meaning of Article 4(1) of Directive [proposal NIS 2];

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

(4) 'cybersecurity' means cybersecurity within the meaning of Article 4(3) of Directive [proposal NIS 2];

(5) 'highest level of management' means a manager, management or coordination and oversight body at the most senior administrative level, taking account of the high-level governance arrangements in each Union institution, body or agency;

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

(7) 'significant incident' means any incident unless it has limited impact and is likely to be already well understood in terms of method or technology;

(8) 'major attack' means any incident requiring more resources than are available at the affected Union institution, body or agency and at CERT-EU;

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

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

(11) 'significant cyber threat' means a cyber threat with the intention, opportunity and capability to cause a significant incident;

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

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

(14) 'cybersecurity risk' means any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems;

(15) 'Joint Cyber Unit' means a virtual and physical platform for cooperation for the different cybersecurity communities in the Union, with a focus on operational and

technical coordination against major cross-border cyber threats and incidents within the meaning of Commission Recommendation of 23 June 2021;

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

Chapter II
MEASURES FOR A HIGH COMMON LEVEL OF CYBERSECURITY

Article 4
Risk management, governance and control

1. Each Union institution, body and agency shall establish its own internal cybersecurity risk management, governance and control framework (‘the framework’) in support of the entity’s mission and exercising its institutional autonomy. This work shall be overseen by the entity’s highest level of management to ensure an effective and prudent management of all cybersecurity risks. The framework shall be in place by …. at the latest [15 months after the entry into force of this Regulation].

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

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

4. Each Union institution, body and agency shall have effective mechanisms in place to ensure that an adequate percentage of the IT budget is spent on cybersecurity.

5. Each Union institution, body and agency shall appoint a Local Cybersecurity Officer or an equivalent function who shall act as its single point of contact regarding all aspects of cybersecurity.

Article 5
Cybersecurity baseline

1. The highest level of management of each Union institution, body and agency shall approve the entity’s own cybersecurity baseline to address the risks identified under the framework referred to in Article 4(1). It shall do so in support of its mission and exercising its institutional autonomy. The cybersecurity baseline shall be in place by …. at the latest [18 months after the entry into force of this Regulation] and shall address the domains listed in Annex I and the measures listed in Annex II.

2. The senior management of each Union institution, body and agency shall follow specific trainings on a regular basis to gain sufficient knowledge and skills in order to apprehend and assess cybersecurity risk and management practices and their impact on the operations of the organisation.

Article 6
Maturity assessments

Each Union institution, body and agency shall carry out a cybersecurity maturity assessment at least every three years, incorporating all the elements of their IT environment as described in Article 4, taking account of the relevant guidance documents and recommendations adopted in accordance with Article 13.

Article 7
Cybersecurity plans

1. Following the conclusions derived from the maturity assessment and considering the assets and risks identified pursuant to Article 4, the highest level of management of each Union institution, body and agency shall approve a cybersecurity plan without undue delay after the establishment of the risk management, governance and control framework and the cybersecurity baseline. The plan shall aim at increasing the overall cybersecurity of the concerned entity and shall thereby contribute to the achievement or enhancement of a high common level of cybersecurity among all Union institutions, bodies and agencies. To support the entity's mission on the basis of its institutional autonomy, the plan shall at least include the domains listed in Annex I, the measures listed in Annex II, as well as measures related to incident preparedness, response and recovery, such as security monitoring and logging. The plan shall be revised at least every three years, following the maturity assessments carried out pursuant to Article 6.
2. The cybersecurity plan shall include staff members' roles and responsibilities for its implementation.
3. The cybersecurity plan shall consider any applicable guidance documents and recommendations issued by CERT-EU.

Article 8
Implementation

1. Upon completion of maturity assessments, the Union institutions, bodies and agencies shall submit these to the Interinstitutional Cybersecurity Board. Upon completion of security plans, the Union institutions, bodies and agencies shall notify the Interinstitutional Cybersecurity Board of the completion. Upon request of the Board, they shall report on specific aspects of this Chapter.
2. Guidance documents and recommendations, issued in accordance with Article 13, shall support the implementation of the provisions laid down in this Chapter.

Chapter III
INTERINSTITUTIONAL CYBERSECURITY BOARD

Article 9
Interinstitutional Cybersecurity Board

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

2. The IICB shall be responsible for:

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

   (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 three representatives nominated by the Union Agencies Network (EUAN) upon a proposal of its ICT Advisory Committee to represent the interests of the agencies and bodies that run their own IT environment and one representative designated by each of the following:

   (a) the European Parliament;

   (b) the Council of the European Union;

   (c) the European Commission;

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

   (e) the European Central Bank;

   (f) the European Court of Auditors;

   (g) the European External Action Service;

   (h) the European Economic and Social Committee;

   (i) the European Committee of the Regions;

   (j) the European Investment Bank;

   (k) the European Union Agency for Cybersecurity.

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

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

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

6. The IICB shall meet at the initiative of its chair, at the request of CERT-EU or at the request of any of its members.

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

8. The IICB may act by a simplified written procedure initiated in accordance with the internal rules of procedure of the IICB. Under that procedure, the relevant decision

shall be deemed approved within the timeframe set by the chair, except where a member objects.

9. The Head of CERT-EU, or his or her alternate, shall participate in IICB meetings except where otherwise decided by the IICB.

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

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

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

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

Article 10
Tasks of the IICB

When exercising its responsibilities, the IICB shall in particular:

(a) review any reports requested from CERT-EU on the state of implementation of this Regulation by the Union institutions, bodies and agencies;

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

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

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

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

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

(g) approve and monitor key performance indicators for CERT-EU defined on a proposal by the Head of CERT-EU;

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

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

Article 11
Compliance

The IICB shall monitor the implementation of this Regulation and of adopted guidance documents, recommendations and calls for action by the Union institutions, bodies and agencies. Where the IICB finds that Union institutions, bodies or agencies have not effectively applied or implemented this Regulation or guidance documents, recommendations and calls for action issued under this Regulation, it may, without prejudice to the internal procedures of the relevant Union institution, body or agency:

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

(b) recommend a relevant audit service to carry out an audit.

Chapter IV
CERT-EU

Article 12
CERT-EU mission and tasks

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

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

   (a) support them with the implementation of this Regulation and contribute to the coordination of the application of this Regulation through the measures listed in Article 13.1 or through ad-hoc reports requested by the IICB;

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

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

   (d) raise to the attention of the IICB any issue relating to the implementation of this Regulation and of the implementation of the guidance documents, recommendations and calls for action;

   (e) report on the cyber threats faced by the Union institutions, bodies and agencies and contribute to the EU cyber situational awareness.

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

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

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

(c) cyber threat intelligence, including situational awareness;

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

4. CERT-EU shall engage in structured cooperation with the European Union Agency for Cybersecurity on capacity building, operational cooperation and long-term strategic analyses of cyber threats in accordance with Regulation (EU) 2019/881 of the European Parliament and of the Council.

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

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

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

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

6. CERT-EU may organise cybersecurity exercises or recommend participation in existing exercises, in close cooperation with the European Union Agency for Cybersecurity whenever applicable, to test the level of cybersecurity of the Union institutions, bodies and agencies.

7. CERT-EU may provide assistance to Union institutions, bodies and agencies regarding incidents in classified IT environments if it is explicitly requested to do so by the constituent concerned.

Article 13

Guidance documents, recommendations and calls for action

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

(a) calls for action describing urgent security measures that Union institutions, bodies and agencies are urged to take within a set timeframe;

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

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

2. Guidance documents and recommendations may include:

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

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

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

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

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

Article 14
Head of CERT-EU

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

Article 15
Financial and staffing matters

1. The Commission, after having obtained the unanimous approval of the IICB, shall appoint the Head of CERT-EU. The IICB shall be consulted at all stages of the procedure prior to the appointment of the Head of CERT-EU, in particular in drafting vacancy notices, examining applications and appointing selection boards in relation to this post.

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

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

4. Union institutions, bodies and agencies other than those referred to in paragraph 3 shall make an annual financial contribution to CERT-EU to cover the services provided by CERT-EU pursuant to that paragraph 3. The respective contributions shall be based on orientations given by the IICB and agreed between each entity and CERT-EU in service level agreements. The contributions shall represent a fair and proportionate share of the total costs of services provided. They shall be received by the distinct budget line referred to in paragraph 3 as assigned revenue as provided for in Article 21(3), point (c) of Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council[8].

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

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

Article 16

Cooperation of CERT-EU with Member State counterparts

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

2. CERT-EU may exchange incident-specific information with national counterparts in the Member States to facilitate detection of similar cyber threats or incidents without the consent of the affected constituent. CERT-EU may only exchange incident-specific information which reveals the identity of the target of the cybersecurity incident with the consent of the affected constituent.

Article 17

Cooperation of CERT-EU with non-Member State counterparts

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

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

3. CERT-EU may, with the consent of the constituent affected by an incident, provide information related to the incident to partners that can contribute to its analysis.

Chapter V
COOPERATION AND REPORTING OBLIGATIONS

Article 18

Information handling

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

2. The provisions of Regulation (EC) No 1049/2001 of the European Parliament and the Council[9] shall apply with regard to requests for public access to documents held

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

by CERT-EU, including the obligation under that Regulation to consult other Union institutions, bodies and agencies whenever a request concerns their documents.

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

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

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

Article 19
Sharing obligations

1. To enable CERT-EU to coordinate vulnerability management and incident response, it may request Union institutions, bodies and agencies to provide it with information from their respective IT system inventories that is relevant for the CERT-EU support. The requested institution, body or agency shall transmit the requested information, and any subsequent updates thereto, without undue delay.

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

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

4. The sharing obligations shall not extend to EU Classified Information (EUCI) and to information that a Union institution, body or agency has received from a Member State Security or Intelligence Service or law enforcement agency under the explicit condition that it will not be shared with CERT-EU.

Article 20
Notification obligations

1. All Union institutions, bodies and agencies shall make an initial notification to CERT-EU of significant cyber threats, significant vulnerabilities and significant incidents without undue delay and in any event no later than 24 hours after becoming aware of them.

   In duly justified cases and in agreement with CERT-EU, the Union institution, body or agency concerned can deviate from the deadline laid down in the previous paragraph.

2. The Union institutions, bodies and agencies shall further notify to CERT-EU without undue delay appropriate technical details of cyber threats, vulnerabilities and incidents that enable detection, incident response or mitigating measures. The notification shall include if available:

(a) relevant indicators of compromise;

(b) relevant detection mechanisms;

(c) potential impact;

(d) relevant mitigating measures.

3. CERT-EU shall submit to ENISA on a monthly basis a summary report including anonymised and aggregated data on significant cyber threats, significant vulnerabilities and significant incidents notified in accordance with paragraph 1.

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

5. The notification obligations shall not extend to EUCI and to information that a Union institution, body or agency has received from a Member State Security or Intelligence Service or law enforcement agency under the explicit condition that it will not be shared with CERT-EU.

Article 21

Incident response coordination and cooperation on significant incidents

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

(a) Union institutions, bodies and agencies;

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

2. CERT-EU shall facilitate coordination among Union institutions, bodies and agencies on incident response, including:

(a) contribution to consistent external communication;

(b) mutual assistance;

(c) optimal use of operational resources;

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

3. CERT-EU shall support Union institutions, bodies and agencies regarding situational awareness of cyber threats, vulnerabilities and incidents.

4. The IICB shall issue guidance on incident response coordination and cooperation for significant incidents. Where the criminal nature of an incident is suspected, CERT-EU shall advise on how to report the incident to law enforcement authorities.

Article 22

Major attacks

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

2. The Union institutions, bodies and agencies shall contribute to the inventory of technical expertise by providing an annually updated list of experts available within their respective organisations detailing their specific technical skills.

3. With the approval of the concerned Union institutions, bodies and agencies, CERT-EU may also call on experts from the list referred to in paragraph 2 for contributing to the response to a major attack in a Member State, in line with the Joint Cyber Unit's operating procedures.

Chapter VI
FINAL PROVISIONS

Article 23
Initial budgetary reallocation

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

Article 24
Review

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

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

3. The Commission shall evaluate the functioning of this Regulation and report to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions no sooner than five years after the date of entry into force.

Article 25
Entry into force

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

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

Done at Brussels,

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

LEGISLATIVE FINANCIAL STATEMENT

1. FRAMEWORK OF THE PROPOSAL/INITIATIVE

1.1. Title of the proposal/initiative

1.2. Policy area(s) concerned

1.3. The proposal/initiative relates to:

1.4. Objective(s)

1.4.1. General objective(s)

1.4.2. Specific objective(s)

1.4.3. Expected result(s) and impact

1.4.4. Indicators of performance

1.5. Grounds for the proposal/initiative

1.5.1. Requirement(s) to be met in the short or long term including a detailed timeline for roll-out of the implementation of the initiative.

1.5.2. Added value of Union involvement (it may result from different factors, e.g. coordination gains, legal certainty, greater effectiveness or complementarities). For the purposes of this point 'added value of Union involvement' is the value resulting from Union intervention which is additional to the value that would have been otherwise created by Member States alone.

1.5.3. Lessons learned from similar experiences in the past

1.5.4. Compatibility with the Multiannual Financial Framework and possible synergies with other appropriate instruments

1.5.5. Assessment of the different available financing options, including scope for redeployment

1.6. Duration and financial impact of the proposal/initiative

1.7. Management mode(s) planned

2. MANAGEMENT MEASURES

2.1. Monitoring and reporting rules

2.2. Management and control system(s)

2.2.1. Justification of the management mode(s), the funding implementation mechanism(s), the payment modalities and the control strategy proposed

2.2.2. Information concerning the risks identified and the internal control system(s) set up to mitigate them

2.2.3. Estimation and justification of the cost-effectiveness of the controls (ratio of 'control costs ÷ value of the related funds managed'), and assessment of the expected levels of risk of error (at payment & at closure)

2.3. Measures to prevent fraud and irregularities

3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE

3.1. Heading(s) of the multiannual financial framework and expenditure budget line(s) affected

3.2. Estimated financial impact of the proposal on appropriations

3.2.1. Summary of estimated impact on operational appropriations

3.2.2. Estimated output funded with operational appropriations

3.2.3. Summary of estimated impact on administrative appropriations

3.2.4. Compatibility with the current multiannual financial framework

3.2.5. Third-party contributions

3.3. Estimated impact on revenue

LEGISLATIVE FINANCIAL STATEMENT

1. FRAMEWORK OF THE PROPOSAL/INITIATIVE

1.1. Title of the proposal/initiative

Proposal for a Regulation of the European Parliament and of the Council laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union

1.2. Policy area(s) concerned

European Public Administration

The proposal concerns measures that ensure a high common level of cybersecurity within the Union institutions, bodies and agencies

1.3. The proposal/initiative relates to:

☑a new action

☐ a new action following a pilot project/preparatory action[10]

☐ the extension of an existing action

☑ a merger or redirection of one or more actions towards another/a new action

1.4. Objective(s)

1.4.1. General objective(s)

– To establish a framework to ensure a high common level of cybersecurity within the Union institutions, bodies and agencies

– To provide a new legal base for CERT-EU to reinforce its mandate and funding

1.4.2. Specific objective(s)

(1) To lay down obligations on Union institutions, bodies and agencies to establish an internal cybersecurity risk management, governance and control framework

(2) To lay down obligations on Union institutions, bodies and agencies to report on their cybersecurity risk management, governance and control framework as well as on cybersecurity incidents

(3) To lay down rules on the organisation and operation of the Cybersecurity Centre for the Union institutions, bodies and agencies (CERT-EU) and on the organisation and operation of the Interinstitutional Cybersecurity Board (IICB)

(4) To contribute to the Joint Cyber Unit

1.4.3. Expected result(s) and impact

Specify the effects which the proposal/initiative should have on the beneficiaries/groups targeted.

– Internal cybersecurity risk management, governance and control frameworks, cybersecurity baselines, regular maturity assessments and cybersecurity plans at the Union institutions, bodies and agencies

[10] As referred to in Article 58(2)(a) or (b) of the Financial Regulation.

– Improvement of cybersecurity resilience and incident response capacities at the Union institutions, bodies and agencies

– Modernisation of CERT-EU

– Contribution to the Joint Cyber Unit

1.4.4. Indicators of performance

Specify the indicators for monitoring progress and achievements.

– Frameworks and baselines in place, regular maturity assessments and cybersecurity plans carried out in the Union institution, bodies and agencies

– Improved handling of incidents

– Increased awareness of cybersecurity risks at the senior management level of the Union institutions, bodies and agencies

– Levelling ICT security spending as a percentage of overall ICT spending

– Strong leadership of the IICB and CERT-EU

– Increased information sharing among the Union institutions, bodies and agencies and with relevant bodies and stakeholders in the EU

– Increased cybersecurity cooperation with relevant bodies and stakeholders in the EU, via CERT-EU and ENISA

1.5. Grounds for the proposal/initiative

1.5.1. Requirement(s) to be met in the short or long term including a detailed timeline for roll-out of the implementation of the initiative.

The proposal aims to increase the level of cyber resilience of the Union institutions, bodies and agencies, to reduce inconsistencies in the resilience across these entities and to improve the level of joint situational awareness and the collective capability to prepare and respond.

The proposal is fully consistent and coherent with other related initiatives, and in particular the proposal for a Directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 [proposal NIS 2].

The proposal is an essential part of the EU Security Union Strategy and the EU's Cybersecurity Strategy for the Digital Decade.

The Regulation is scheduled to be proposed by the European Commission in October 2021, the adoption of the Regulation by the European Parliament and the Council is expected in 2022 and the provisions will be applicable from the entry into force of the Regulation. The financial and HR impact outlined in this Legislative Financial Statement are foreseen to begin in 2023. A preparatory period has already begun in 2021, but the preparatory activities in 2021 and 2022 are outside the financial impact of the proposal.

1.5.2. Added value of Union involvement (it may result from different factors, e.g. coordination gains, legal certainty, greater effectiveness or complementarities). For the purposes of this point 'added value of Union involvement' is the value resulting from Union intervention which is additional to the value that would have been otherwise created by Member States alone.

Reasons for action at European level (ex-ante)

From 2019 to 2021, the number of significant incidents affecting Union institutions, bodies and agencies, authored by advanced persistent threat actors, has surged dramatically. The first half of 2021 saw the equivalent in significant incidents as in the whole of 2020. This is as well reflected in the number of forensics images (snapshots of the contents of affected systems or devices) CERT-EU analysed in 2020, which tripled in comparison to 2019, while the number of significant incidents rose more than ten-fold since 2018.

The levels of cybersecurity maturity vary substantially from one entity to another[11]. This Regulation ensures that all Union institutions, bodies and agencies will implement a baseline of security measures and cooperate among each other with as its goal the open and efficient functioning of the Union administration.

The systems to be preserved fall within the autonomy of and are operated by the Union institutions, bodies and agencies; the proposed actions could not be created by the Member States.

1.5.3. Lessons learned from similar experiences in the past

The NIS Directive has been the first horizontal internal market instrument aimed at improving the resilience of networks and systems in the Union against cybersecurity risks. Since its entry into force in 2016, it has contributed greatly to raising the common level of cybersecurity amongst the Member States. The proposal for the NIS2 Directive seeks to further improve these measures.

The Regulation seeks to provide similar measures for the Union institutions, bodies and agencies.

1.5.4. Compatibility with the Multiannual Financial Framework and possible synergies with other appropriate instruments

The proposal is consistent with the Multiannual Financial Framework and is an essential part of the EU Security Union Strategy as well as the EU's Cybersecurity Strategy for the Digital Decade.

The proposal envisages to apply measures for a high common level of cybersecurity to Union institutions, bodies and agencies. The proposal is in line with the proposal for a Directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 [proposal NIS 2].

1.5.5. Assessment of the different available financing options, including scope for redeployment

The management of the tasks by CERT-EU necessitate specific profiles and supplementary workload that cannot be absorbed without any increase of human and financial resources.

[11] Reference: [ECA Special Report on cybersecurity at the Union institutions, bodies and agencies].

1.6. Duration and financial impact of the proposal/initiative

☐ **limited duration**

– ☐ in effect from [DD/MM]YYYY to [DD/MM]YYYY

– ☐ Financial impact from YYYY to YYYY for commitment appropriations and from YYYY to YYYY for payment appropriations.

☑ **unlimited duration**

– The financial impact should start with the first budget adopted following the entry into force of the Regulation. A reallocation of resources from the Union institutions and main bodies to the Commission would take place in the first year, considered a transition year; this and other (re)allocation of resources will take place in the framework of the annual budgets. If the Regulation is adopted in 2022, financial year 2023 will be the transitory period, and 2024 will operate at full-scale.

1.7. Management mode(s) planned[12]

☑ **Direct management** by the Commission and by each Union institution, body and agency

– ☑ by its departments, including by its staff in the Union delegations;

– ☐ by the executive agencies

☐ **Shared management** with the Member States

☐ **Indirect management** by entrusting budget implementation tasks to:

– ☐ third countries or the bodies they have designated;

– ☐ international organisations and their agencies (to be specified);

– ☐ the EIB and the European Investment Fund;

– ☐ bodies referred to in Articles 70 and 71 of the Financial Regulation;

– ☐ public law bodies;

– ☐ bodies governed by private law with a public service mission to the extent that they provide adequate financial guarantees;

– ☐ bodies governed by the private law of a Member State that are entrusted with the implementation of a public-private partnership and that provide adequate financial guarantees;

– ☐ persons entrusted with the implementation of specific actions in the CFSP pursuant to Title V of the TEU, and identified in the relevant basic act.

– *If more than one management mode is indicated, please provide details in the 'Comments' section.*

Comments

For the application of administrative and financial procedures, CERT-EU acts under the authority of the Commission.

Additional resources stemming from the draft Regulation:

[12] Details of management modes and references to the Financial Regulation may be found on the BudgWeb site: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx

The implementation of Article 12 and 13 of the draft Regulation leads to an enlarged service catalogue with additional baseline services. When operating at full-scale, the following additional resources will be necessary (until the end of the MFF at the end of 2027): 21 FTE and EUR 14.05 million.

The breakdown of the additional resources under the budget over the different tasks is as follows:

(a) For the performance of tasks for the Union institutions, bodies and agencies detailed in Article 12.2 (a), (b), (c), and (e): 13.75 FTE and EUR 11.275 million;

(b) For the performance of tasks detailed in Article 12.3 (contribution to Joint Cyber Unit): 2 FTE and EUR 381 000;

(c) For the performance of tasks detailed in Article 12.4 (structured cooperation with ENISA): 0.25 FTE and EUR 236 000;

(d) For the performance of tasks detailed in Article 12.6 (cybersecurity exercises): 0.25 FTE and EUR 79 000;

(e) For performance of tasks detailed in Article 12.2 (d) and Article 13 (analysis and reporting on implementation of the Regulation, preparation of guidance documents, recommendations and calls for action): 3.75 FTE and EUR 2.079 million.

(f) For the performance of tasks to support the secretariat of the Interinstitutional Cybersecurity Board (IICB): 1 FTE.

Overview of current resources and transition to full scale:

In September 2021 CERT-EU operated with the following resources:

- permanent and seconded posts: 14 FTEs,

- contract agents financed under service level agreements: 24 FTE,

- total 38 FTE.

CERT-EU budget in 2020 was: EUR 250 000 under the Commission Budget, EUR 3.5 million through assigned revenues from service level agreements. Total: EUR 3.75 million. This constituted the entire CERT-EU budget covering training, hardware, software, missions, support, contract agents and conferences.

Once the regulation is into force the future resources of CERT-EU are foreseen to be:

- permanent posts: 34 FTE,

- contract agents: 15 FTE,

- total 49 FTE, thus a net increase of 11 FTE.

The change in ratio between permanent posts and contract agents addresses the pertinent stumbling block of hiring and retaining senior cybersecurity professionals due to their scarcity on the labour market.

In addition, 1 FTE contract agent will be required within the Commission's Directorate-General for Informatics to support the IICB (Interinstitutional Cybersecurity Board).

In total 21 FTE additional will thus be required to implement the Regulation (20 FTE for CERT-EU and 1 for the Commission's Directorate-General for Informatics). This will be compensated by a parallel reduction of 9 FTE contract agents in CERT-EU which were previously financed through assigned revenue from service level agreements.

The CERT-EU non-human resources budget in 2024 after transition period will cover the tasks listed above under (a) through (e) and is foreseen to be funded as follows:

- EUR 8.921 million per year from the Union institutions financed under Union budget Heading 7,

- EUR 2.459 million from Union institutions, bodies and agencies financed under Union budget Headings 1 to 6,

- EUR 2.670 million from self-financed Union institutions, bodies and agencies.

- Total CERT-EU budget: EUR 14.05 million.

The tasks listed in Article 12.5 are not described in its service catalogue, these are chargeable services. These are ancillary, represent relatively low amounts, are mostly temporary, and the costs of these services will be recovered from beneficiaries of the services through service level agreements or written agreements.

With regards to contributions to staff of CERT-EU: the Union institutions and main bodies shall contribute a fair share which is in proportion to the respective share of permanent AD posts of the organisation. It should be seen whether ECB and EIB can also contribute a fair share through secondment of permanent staff.

2. MANAGEMENT MEASURES

2.1. Monitoring and reporting rules

Specify frequency and conditions.

The Commission, with the help of the IICB and CERT-EU, will periodically review the functioning of the Regulation and report to the European Parliament and the Council, the first time no later than 48 months after the entry into force of this Regulation, and thereafter every three years.

The data sources used for the reviews would mostly be from the IICB and CERT-EU. In addition, specific data gathering tools could be used when needed, e.g. surveys of the Union institutions, bodies and agencies, ENISA or the CSIRTs Network.

2.2. Management and control system(s)

2.2.1. Justification of the management mode(s), the funding implementation mechanism(s), the payment modalities and the control strategy proposed

Actions deriving from the Regulation will be managed within each Union institution, body and agency in accordance with their relevant applicable rules and regulations.

Administrative and financial management of CERT-EU activities is embedded within the Commission administration and follows its applicable management and implementation mechanisms, payment modalities and controls.

The Commission's internal auditor exercises the same powers over CERT-EU as over the Commission departments.

2.2.2. Information concerning the risks identified and the internal control system(s) set up to mitigate them

Very low risk, as CERT-EU is already attached administratively as a Commission Taskforce to the Director-General for Informatics, and the IICB is modelled on the current CERT-EU Steering Board. The ecosystem for financial management and internal control is thus already in place.

2.2.3. Estimation and justification of the cost-effectiveness of the controls (ratio of 'control costs ÷ value of the related funds managed'), and assessment of the expected levels of risk of error (at payment & at closure)

Procedures for procurement, financial management and control are already in place and well tested. Cost-effectiveness of controls and the levels of risk of error correspond to those in each Union institution, body or agency, and to those of the Commission for CERT-EU activities.

2.3. Measures to prevent fraud and irregularities

Specify existing or envisaged prevention and protection measures, e.g. from the Anti-Fraud Strategy.

The financial management and internal control systems of the Commission apply for CERT-EU activities.

In order to combat fraud, corruption and other unlawful activities the provisions of Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-fraud Office (OLAF) applies without restriction.

3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE

3.1. Heading(s) of the multiannual financial framework and expenditure budget line(s) affected

- Existing budget lines

In order of multiannual financial framework headings and budget lines.

Heading of multiannual financial framework	Budget line	Type of expenditure	Contribution			
	Number	Diff./Non-diff.[13]	from EFTA countries [14]	from candidate countries[15]	from third countries	within the meaning of Article 21(2)(b) of the Financial Regulation
1 to 6	Budget lines covering Union contributions to decentralised agencies and bodies	Diff.	NO	NO	NO	NO
7	Budget lines covering staff remunerations, IT expenditure and other administrative expenditure in the different Sections of the EU budget	Non-diff.	NO	NO	NO	NO

- New budget lines requested

In order of multiannual financial framework headings and budget lines.

Heading of multiannual financial framework	Budget line	Type of expenditure	Contribution			
	Number	Diff./Non-diff.	from EFTA countries	from candidate countries	from third countries	within the meaning of Article 21(2)(b) of the Financial Regulation
	None		YES/NO	YES/NO	YES/NO	YES/NO

[13] Diff. = Differentiated appropriations / Non-diff. = Non-differentiated appropriations.
[14] EFTA: European Free Trade Association.
[15] Candidate countries and, where applicable, potential candidates from the Western Balkans.

3.2. Estimated financial impact of the proposal on appropriations

3.2.1. Summary of estimated impact on operational appropriations

– ☐ The proposal/initiative does not require the use of operational appropriations

– ☑ The proposal/initiative requires the use of operational appropriations, as explained below:

EUR million (to three decimal places)

Heading of multiannual financial framework	1 to 6	Headings covering contributions to decentralised agencies and bodies

DG: Several			Year **2023**	Year **2024**	Year **2025**	Year **2026**	Year **2027**	**TOTAL**
○ Operational appropriations								
Budget lines covering Union contributions to decentralised agencies (xx 10 xx xx)[16]	Commitments	(1a)	2.459	2.459	2.459	2.459	2.459	12.293
	Payments	(2a)	2.459	2.459	2.459	2.459	2.459	12.293
Appropriations of an administrative nature financed from the envelope of specific programmes[17]								
Budget line		(3)						
TOTAL appropriations for DG: Several	Commitments	=1a+1b +3	2.459	2.459	2.459	2.459	2.459	12.293
	Payments	=2a+2b +3	2.459	2.459	2.459	2.459	2.459	12.293

[16] According to the official budget nomenclature.

[17] Technical and/or administrative assistance and expenditure in support of the implementation of EU programmes and/or actions (former 'BA' lines), indirect research, direct research.

○ TOTAL operational appropriations	Commitments	(4)	2.459	2.459	2.459	2.459	2.459	12.293
	Payments	(5)	2.459	2.459	2.459	2.459	2.459	12.293
○ TOTAL appropriations of an administrative nature financed from the envelope for specific programmes		(6)						
TOTAL appropriations under HEADINGS 1 to 6 of the multiannual financial framework	Commitments	=4+ 6	2.459	2.459	2.459	2.459	2.459	12.293
	Payments	=5+ 6	2.459	2.459	2.459	2.459	2.459	12.293

If more than one operational heading is affected by the proposal / initiative, repeat the section above:

○ TOTAL operational appropriations (all operational headings)	Commitments	(4)	2.459	2.459	2.459	2.459	2.459	12.293
	Payments	(5)	2.459	2.459	2.459	2.459	2.459	12.293
TOTAL appropriations of an administrative nature financed from the envelope for specific programmes (all operational headings)		(6)						
TOTAL appropriations under HEADINGS 1 to 6 of the multiannual financial framework (Reference amount)	Commitments	=4+ 6	2.459	2.459	2.459	2.459	2.459	12.293
	Payments	=5+ 6	2.459	2.459	2.459	2.459	2.459	12.293

Heading of multiannual financial framework	**7**	'Administrative expenditure'

This section should be filled in using the 'budget data of an administrative nature' to be firstly introduced in the Annex to the Legislative Financial Statement (Annex V to the internal rules), which is uploaded to DECIDE for interservice consultation purposes.

EUR million (to three decimal places)

		Year **2023**	Year **2024**	Year **2025**	Year **2026**	**Year 2027**	**TOTAL**
DG: DIGIT (CERT-EU)							
○ Human resources		1.184	2.126	2.754	3.225	3.225	12.514
○ Other administrative expenditure		7.938	8.921	8.921	8.921	8.921	43.622
TOTAL DG DIGIT (CERT-EU)	Appropriations	9.122	11.047	11.675	12.146	12.146	56.136

TOTAL appropriations under HEADING 7 of the multiannual financial framework	(Total commitments = Total payments)	9.122	11.047	11.675	12.146	12.146	**56.136**

EUR million (to three decimal places)

		Year 2023	Year 2024	Year 2025	Year 2026	Year 2027	**TOTAL**
TOTAL appropriations under HEADINGS 1 to 7 of the multiannual financial framework (*)	Commitments	11.581	13.506	14.134	14.605	14.605	68.429
	Payments	11.581	13.506	14.134	14.605	14.605	68.429

(*) Contributions from self-financed Union institutions, bodies and agencies are estimated at EUR 2.670 million per year (total for the five years, EUR 13.350 million). The contributions will constitute assigned revenues for CERT-EU. The tables above only include the estimated total impact on the Union budget and do not include those contributions.

3.2.2. Estimated output funded with operational appropriations

Commitment appropriations in EUR million (to three decimal places)

Indicate objectives and outputs ⇩			Year **N**		Year **N+1**		Year **N+2**		Year **N+3**		Enter as many years as necessary to show the duration of the impact (see point 1.6)						**TOTAL**	
	OUTPUTS																	
	Type[18]	Average cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	Total No	Total cost
SPECIFIC OBJECTIVE No 1[19]…																		
- Output																		
- Output																		
- Output																		
Subtotal for specific objective No 1																		
SPECIFIC OBJECTIVE No 2 ...																		
- Output																		
Subtotal for specific objective No 2																		
TOTALS																		

[18] Outputs are products and services to be supplied (e.g.: number of student exchanges financed, number of km of roads built, etc.).

[19] As described in point 1.4.2. 'Specific objective(s)…'

3.2.3. Summary of estimated impact on administrative appropriations

– ☐ The proposal/initiative does not require the use of appropriations of an administrative nature

– ☑ The proposal/initiative requires the use of appropriations of an administrative nature, as explained below:

EUR million (to three decimal places)

	Year 2023	Year 2024	Year 2025	Year 2026	Year 2027	**TOTAL**
HEADING 7 of the multiannual financial framework						
Human resources						
Permanent staff (AD Grades)	1.099	2.041	2.669	3.14	3.14	12.089
Contract staff	0.085	0.085	0.085	0.085	0.085	0.425
Other administrative expenditure	7.938	8.921	8.921	8.921	8.921	43.622
Subtotal HEADING 7 of the multiannual financial framework	9.122	11.047	11.675	12.146	12.146	56.136

Outside HEADING 7[20] of the multiannual financial framework						
Human resources						
Other expenditure of an administrative nature						
Subtotal outside HEADING 7 of the multiannual financial framework						

TOTAL	9.122	11.047	11.675	12.146	12.146	56.136

The appropriations required for human resources and other expenditure of an administrative nature will be met by appropriations from the DG that are already assigned to management of the action and/or have been redeployed within the DG, together if necessary with any additional allocation which may be granted to the managing DG under the annual allocation procedure and in the light of budgetary constraints.

[20] Technical and/or administrative assistance and expenditure in support of the implementation of EU programmes and/or actions (former 'BA' lines), indirect research, direct research.

3.2.3.1. Estimated requirements of human resources

– ☐ The proposal/initiative does not require the use of human resources.

– ☑ The proposal/initiative requires the use of human resources, as explained below:

Estimate to be expressed in full time equivalent units

		Year 2023	Year 2024	Year 2025	Year 2026	Year 2027		
O Establishment plan posts (officials and temporary staff)								
20 01 02 01 (Headquarters and Commission's Representation Offices)		7	13	17	20	20		
20 01 02 03 (Delegations)								
01 01 01 01 (Indirect research)								
01 01 01 11 (Direct research)								
Other budget lines (specify)								
O External staff (in Full Time Equivalent unit: FTE)[21]								
20 02 01 (AC, END, INT from the 'global envelope')		1	1	1	1	1		
20 02 03 (AC, AL, END, INT and JPD in the delegations)								
XX 01 xx **yy zz** [22]	- at Headquarters							
	- in Delegations							
01 01 01 02 (AC, END, INT - Indirect research)								
01 01 01 12 (AC, END, INT - Direct research)								
Other budget lines (specify)								
TOTAL		**8**	**14**	**18**	**21**	**21**		

XX is the policy area or budget title concerned.

The human resources required will be met by staff from the DG who are already assigned to management of the action and/or have been redeployed within the DG, together if necessary with any additional allocation which may be granted to the managing DG under the annual allocation procedure and in the light of budgetary constraints.

Description of tasks to be carried out:

Officials and temporary staff	Officials will implement the tasks and activities of CERT-EU as per the Regulation, in particular Chapters IV and V.
External staff	The Contractual Agent will assist the secretarial functions of the Interinstitutional Cybersecurity Board.

[21] AC= Contract Staff; AL = Local Staff; END= Seconded National Expert; INT = agency staff; JPD= Junior Professionals in Delegations.

[22] Sub-ceiling for external staff covered by operational appropriations (former 'BA' lines).

3.2.4. Compatibility with the current multiannual financial framework

The proposal/initiative:

– ☑ can be fully financed through redeployment within the relevant heading of the Multiannual Financial Framework (MFF).

Explain what reprogramming is required, specifying the budget lines concerned and the corresponding amounts. Please provide an excel table in the case of major reprogramming.

– ☐ requires use of the unallocated margin under the relevant heading of the MFF and/or use of the special instruments as defined in the MFF Regulation.

Explain what is required, specifying the headings and budget lines concerned, the corresponding amounts, and the instruments proposed to be used.

– ☐ requires a revision of the MFF.

Explain what is required, specifying the headings and budget lines concerned and the corresponding amounts.

3.2.5. Third-party contributions

The proposal/initiative:

– ☑ does not provide for co-financing by third parties[23]

– ☐ provides for the co-financing by third parties estimated below:

Appropriations in EUR million (to three decimal places)

	Year **N**[24]	Year **N+1**	Year **N+2**	Year **N+3**	Enter as many years as necessary to show the duration of the impact (see point 1.6)			Total
Specify the co-financing body								
TOTAL appropriations co-financed								

[23] The assigned revenues steaming from the sporadic provision of services to non-constituent organisations foreseen in Article 12.5(c) have not been estimated because should be marginal.

[24] Year N is the year in which implementation of the proposal/initiative starts. Please replace 'N' by the expected first year of implementation (for instance: 2021). The same for the following years.

3.3. Estimated impact on revenue

– ☑ The proposal/initiative has no financial impact on revenue.

– ☐ The proposal/initiative has the following financial impact:

– ☐ on own resources

– ☐ on other revenue

– please indicate, if the revenue is assigned to expenditure lines ☐

EUR million (to three decimal places)

Budget revenue line:	Appropriations available for the current financial year	Impact of the proposal/initiative[25]						
		Year **N**	Year **N+1**	Year **N+2**	Year **N+3**	Enter as many years as necessary to show the duration of the impact (see point 1.6)		
Article …….								

For assigned revenue, specify the budget expenditure line(s) affected.

Other remarks (e.g. method/formula used for calculating the impact on revenue or any other information).

[25] As regards traditional own resources (customs duties, sugar levies), the amounts indicated must be net amounts, i.e. gross amounts after deduction of 20 % for collection costs.

EUROPEAN
COMMISSION

Brussels, 22.3.2022
COM(2022) 122 final

ANNEXES 1 to 2

ANNEXES

to the

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

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

{SWD(2022) 67 final} - {SWD(2022) 68 final}

ANNEX I

The following domains shall be addressed in the cybersecurity baseline:

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

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

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

(4) access control;

(5) operations security;

(6) communications security;

(7) system acquisition, development and maintenance;

(8) supplier relationships;

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

(10) business continuity management and crisis management; and

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

ANNEX II

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

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

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

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

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

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

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

Information Note

1. Proposal
Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union

2. Date of Commission document
22/03/2022

3. Number of Commission document
COM (2022) 122 Final

4. Number of Council document:
2022/0085 (COD)

5. Dealt with in Brussels by
Telecommunications Council / Horizontal Working Party on Cyber Issues

6. Department with primary responsibility
Department of the Environment, Climate and Communications

7. Other Departments involved
None

8. Background to, short summary and aim of the proposal
Background to Proposal
This proposal builds on the EU Security Union Strategy (COM(2020) 605 final) and the EU's Cybersecurity Strategy for the Digital Decade (JOIN(2020) 18 final).
CERT-EU has conducted an assessment of the principal cyber threats to which Union institutions, bodies and agencies are currently exposed or are likely to be exposed to in the foreseeable future. Three categories of observations were used in the analysis:

- *Attempts to breach Union institutions, bodies and agencies' IT infrastructure (when successful, they are treated as incidents, in the other cases they are still recorded as detected attempts).*
- *Threats detected in the proximity of Union institutions, bodies and agencies (e.g. in their related sectors, their stakeholder communities or in Europe).*
- *Major threat trends observed globally.*

Furthermore, the analysis considered how major ongoing shifts are affecting the ways in which Union institutions manage and use their IT infrastructure and services. Such shifts include:

- *Increased teleworking.*
- *Migration of systems to the cloud.*
- *Increased outsourcing of IT services.*

From 2019 to 2021, the number of significant incidents1 affecting Union institutions, bodies and agencies, authored by advanced persistent threat (APT) actors, has surged dramatically. The first half of 2021 saw the equivalent in significant incidents as in the whole of 2020.

Summary of Proposal

This proposal establishes a framework for ensuring common cybersecurity rules and measures among the Union institutions, bodies and agencies. It aims at further improving all entities' resilience and incident response capacities. It is in line with the Commission's priorities to make Europe fit for the digital age and to build a future-ready economy that works for the people. Moreover, ensuring a secure and resilient public administration is a cornerstone in the digital transformation of society as a whole. The proposal modernises the existing CERT-EU legal framework and takes account of the changed and increased digitisation of the institutions, bodies and agencies in recent years as well as the evolving cybersecurity threat landscape.

Aims of Proposal

- *To place an obligation on Union institutions, bodies and agencies to establish an internal cybersecurity risk management, governance and control framework that ensures an effective and prudent management of all cybersecurity risks.*
- *To establish a mandatory cybersecurity baseline for the institutions, bodies and agencies to address the risks identified under the framework, carry out regular cybersecurity maturity assessments and adopt a cybersecurity plan.*
- *To establish an Interinstitutional Cybersecurity Board with responsibility for monitoring the implementation of this Regulation by the Union institutions, bodies and agencies as well as supervising the implementation of general priorities and objectives by CERT-EU and providing strategic direction to CERT-EU.*
- *To mandate CERT-EU with contributing to the security of the IT environment of all Union institutions, bodies and agencies by advising them, by helping to prevent, detect, mitigate and respond to incidents and by acting as their cybersecurity information exchange and incident response coordination hub.*
- *To ensure cooperation and the exchange of information among CERT-EU, and the Union institutions, bodies and agencies to develop trust and confidence.*
- *To place an obligation on all Union institutions, bodies and agencies to notify CERT-EU of significant cyber threats, significant vulnerabilities and significant incidents without undue delay and in any event no later than 24 hours after becoming aware of them.*

9. Legal basis of the proposal

The legal basis for this Regulation is Article 298 of the Treaty on the Functioning of the European Union (TFEU) which provides that in carrying out their missions, the institutions, bodies, offices and agencies of the Union shall have the support of an open, efficient and independent European administration. In compliance with the Staff Regulations and the Conditions of Employment adopted on the basis of Article 336, the European Parliament and the Council, acting by means of regulations in accordance with the ordinary legislative procedure, shall establish provisions to that end.

10. Voting Method

QMV

11. Role of the EP
Co-Decision

12. Category of proposal
Little Significance

13. Implications for Ireland & Ireland's Initial View

Few implications for Ireland. Ireland supports the measure

14. Impact on the public?

Enhanced cyber security of EU institutions, bodies and agencies will help to protect personal data and enhance public trust.

15. Have consultations with Stakeholders taken place or are there any plans to do so?

The Commission has consulted stakeholders throughout the Union institutions, bodies and agencies as well as representatives of Member States in the Council and stakeholders in the European Parliament. On 25 June 2021, representatives of Member States and relevant stakeholders from the Union institutions, bodies and agencies participated in a workshop organised by the Commission to discuss the content of the future proposal for Regulation.

16. Are there any subsidiarity issues for Ireland?
No.

17. Anticipated negotiating period
12-18 months

18. Proposed implementation date
Q3 2023

19. Consequences for national legislation
Brief description of implementation measures

20. Method of Transposition into Irish law
Regulation becomes directly applicable upon signature – no transposition required

21. Anticipated Transposition date
See above

22. Consequences for the EU budget in Euros annually
The Commission is unable to project the anticipated cost of implementing the Regulation due to the lack of detailed information on IT expenditure of the Union institutions, bodies and agencies and the relevant share of cybersecurity spending. The Commission's assessment is that it is likely that many Union institutions, bodies and agencies currently spend less on cybersecurity than they should. However the Commission does not believe this Regulation will not cause as such an increase in that current expenditure as even without the Regulation each

entity would need to ensure an adequate level of cybersecurity.
CERT-EU will require additional resources to fulfil its expanded role and these resources should be reallocated from the Union institutions, bodies and agencies benefitting from CERT-EU's services.

23. Contact name, telephone number and e-mail address of official in Department with primary responsibility?
Peter Hogan, 0879739846, Peter.Hogan@decc.gov.ie

21 April 2022