Council of the European Union

Brussels, 17 December 2020
(OR. en)

14150/20

Interinstitutional File:
2020/0359(COD)

CYBER 281
JAI 1119
DATAPROTECT 155
TELECOM 270
MI 581
CSC 368
CSCI 97

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	16 December 2020
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	COM(2020) 823 final
Subject:	Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148

Delegations will find attached document COM(2020) 823 final.

Encl.: COM(2020) 823 final

EUROPEAN
COMMISSION

Brussels, 16.12.2020
COM(2020) 823 final

2020/0359 (COD)

Proposal for a

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148

(Text with EEA relevance)

{SEC(2020) 430 final} - {SWD(2020) 344 final} - {SWD(2020) 345 final}

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

• Reasons for and objectives of the proposal

This proposal is part of a package of measures to improve further the resilience and incident response capacities of public and private entities, competent authorities and the Union as a whole in the field of cybersecurity and critical infrastructure protection. 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. Cybersecurity is a priority in the Commission's response to the COVID-19 crisis. The package includes a new Strategy on Cybersecurity with the aim of strengthening the Union's strategic autonomy to improve its resilience and collective response and to build an open and global internet. Finally, the package contains a proposal for a directive on the resilience of critical operators of essential services, which aims to mitigate physical threats against such operators.

This proposal builds on and repeals Directive (EU) 2016/1148 on security of network and information systems (NIS Directive), which is the first piece of EU-wide legislation on cybersecurity and provides legal measures to boost the overall level of cybersecurity in the Union. The NIS Directive has (1) contributed to improving cybersecurity capabilities at national level by requiring Member States to adopt national cybersecurity strategies and to appoint cybersecurity authorities; (2) increased cooperation between Member States at Union level by setting up various fora facilitating the exchange of strategic and operational information; and (3) improved the cyber resilience of public and private entities in seven specific sectors (energy, transport, banking, financial market infrastructures, healthcare, drinking water supply and distribution, and digital infrastructures) and across three digital services (online marketplaces, online search engines and cloud computing services) by requiring Member States to ensure that operators of essential services and digital service providers put in place cybersecurity requirements and report incidents.

The proposal modernises the existing legal framework taking account of the increased digitisation of the internal market in recent years and an evolving cybersecurity threat landscape. Both developments have been further amplified since the onset of the COVID-19 crisis. The proposal also addresses several weaknesses that prevented the NIS Directive from unlocking its full potential.

Notwithstanding its notable achievements, the NIS Directive, which paved the way for a significant change in mind-set, in relation to the institutional and regulatory approach to cybersecurity in many Member States, has also proven its limitations. The digital transformation of society (intensified by the COVID-19 crisis) has expanded the threat landscape and is bringing about new challenges which require adapted and innovative responses. The number of cyber -attacks continues to rise, with increasingly sophisticated attacks coming from a wide range of sources inside and outside the EU.

The evaluation on the functioning of the NIS Directive, conducted for the purposes of the Impact Assessment, identified the following issues: (1) the low level of cyber resilience of businesses operating in the EU; (2) the inconsistent resilience across Member States and sectors; and (3) the low level of joint situational awareness and lack of joint crisis response. For example, certain major hospitals in a Member State do not fall within the scope of the NIS Directive and hence are not required to implement the resulting security measures, while in another Member State almost every single healthcare provider in the country is covered by the NIS security requirements.

Being an initiative within the Regulatory Fitness Programme (REFIT), the proposal aims at reducing the regulatory burden for competent authorities and compliance costs for public and private entities. Most notably, this is achieved by abolishing the obligation of competent authorities to identify operators of essential services and by increasing the level of harmonisation of security and reporting requirements to facilitate regulatory compliance for entities providing cross-border services. At the same time, competent authorities will also be given a number of new tasks, including the supervision of entities in sectors so far not covered by the NIS Directive.

- **Consistency with existing policy provisions in the policy area**

This proposal is part of a wider set of existing legal instruments and upcoming initiatives at Union level aimed at increasing the resilience of public and private entities against threats.

In the area of cybersecurity, these are notably Directive (EU) 2018/1972 establishing the European Electronic Communications Code (the cybersecurity-related provisions of which will be replaced by the provisions of the proposal at hand) and the proposal for a Regulation on digital operational resilience for the financial sector (COM(2020) 595 final), which will be considered as *lex specialis* to the proposal at hand once both acts have come into force.

In the area of physical security, the proposal complements the proposal for a Directive on the resilience of critical entities, which revises Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (ECI Directive), which establishes a Union process for identifying and designating European critical infrastructures, and sets out an approach for improving their protection. In July 2020, the Commission adopted the EU Security Union Strategy[1], which acknowledged the increasing interconnection and interdependency between physical and digital infrastructures. It underlined the need for a more coherent and consistent approach between the ECI Directive and the Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union.

The proposal is therefore closely aligned with the proposal for a Directive on the resilience of critical entities, which aims at enhancing the resilience of critical entities against physical threats in a large number of sectors. The proposal aims to ensure that competent authorities under both legal acts take complementary measures and exchange information as necessary regarding cyber and non-cyber resilience, and that particularly critical operators in the sectors considered to be 'essential' per the proposal at hand are also subject to more general resilience-enhancing obligations with an emphasis on non-cyber risks.

- **Consistency with other Union policies**

As set-out in the Communication 'Shaping Europe's digital future'[2], it is crucial for Europe to reap all the benefits of the digital age and to strengthen its industry and innovation capacity, within safe and ethical boundaries. The European strategy for data sets out four pillars – data protection, fundamental rights, safety and cybersecurity – as essential pre-requisites for a society empowered by the use of data.

1 COM(2020)605 final.
2 COM(2020)67 final.

In a resolution from 12 March 2019, the European Parliament called *"[...] on the Commission to assess the need to further enlarge the scope of the NIS Directive to other critical sectors and services that are not covered by sector-specific legislation"*.[3] The Council, in its conclusions from 9 June 2020, welcomed "*[...] the Commission's plans to ensure consistent rules for market operators and facilitate secure, robust and appropriate information-sharing on threats as well as incidents, including through a review of the Directive on security of network and information systems (NIS Directive), to pursue options for improved cyber resilience and more effective responses to cyber-attacks, particularly on essential economic and societal activities, whilst respecting Member States' competences, including the responsibility for their national security."*[4] Furthermore, the proposed legal act is without prejudice to the application of competition rules laid down in the Treaty on the Functioning of the European Union (TFEU).

Given that a significant part of the cybersecurity threats have their origin outside of the EU, a coherent approach to international cooperation is needed. This Directive shall constitute a reference model to be promoted in the context of the EU's cooperation with third countries, notably when providing external technical assistance.

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

• Legal basis

The legal basis for the NIS Directive is Article 114 of the Treaty on the Functioning of the European Union, whose objective is the establishment and functioning of the internal market by enhancing measures for the approximation of national rules. As held by the Court of Justice of the EU in its judgement in Case C-58/08 Vodafone and others, the resort to Article 114 TFEU is justified where there are differences between national rules which have a direct effect on the functioning of the internal market. Equally, the Court held that where an act based on Article 114 TFEU has already removed any obstacle to trade in the area that it harmonises, the Union legislature cannot be denied the possibility of adapting that act to any change in circumstances or development of knowledge having regard to its task of safeguarding the general interests recognised by the Treaty. Finally, the Court held that the measures for the approximation covered by article 114 TFEU are intended to allow a margin of discretion, depending on the general context and the specific circumstances of the matter to be harmonised, as to the method of approximation most appropriate to achieve the desired result. The proposed legal act would remove obstacles to, and improve the establishment and functioning of the internal market for essential and important entities by: establishing clear generally applicable rules on the scope of application of the NIS Directive, harmonising the rules applicable in the area of cybersecurity risk management and incident reporting. Current disparities in this area, both at legislative and supervisory levels, as well as national and EU levels, are obstacles to the internal market because entities that engage in cross-border activities face different, and possibly overlapping, regulatory requirements and/or their application, to the detriment of the exercise of their freedoms of establishment and of provision of services. Different rules also have a negative impact on the conditions of competition in the internal market when it comes to entities of the same type in different Member States.

[3] https://www.europarl.europa.eu/doceo/document/TA-8-2019-0156_EN.html
[4] https://data.consilium.europa.eu/doc/document/ST-8711-2020-INIT/en/pdf

- **Subsidiarity (for non-exclusive competence)**

Cybersecurity resilience across the Union cannot be effective if approached in a disparate manner through national or regional silos. The NIS Directive partly addressed this shortcoming, by setting a framework for network and information systems security at national and Union levels. However, its transposition and implementation also brought to light inherent shortcomings and limits of certain provisions or approaches, such as the unclear delimitation of the scope of the directive leading to significant differences in the extent and depth of de facto EU intervention at Member State level. Furthermore, since the COVID-19 crisis, the European economy has grown even more dependent on network and information systems than ever before and sectors and services are increasingly interconnected. EU intervention going beyond the current measures of the NIS Directive is justified mainly by: (i) the increasingly cross-border nature of the NIS-related threats and challenges; (ii) the potential of Union's action to improve and facilitate effective and coordinated national policies; and (iii) the contribution of concerted and collaborative policy actions to effective protection of data protection and privacy.

- **Proportionality**

The rules proposed in this Directive do not go beyond what is necessary to meet the specific objectives satisfactorily. The envisaged alignment and streamlining of security measures and reporting obligations relate to Member States and businesses' requests to improve the current framework.

The proposal takes account of the already existing practices in the Member States. An enhanced level of protection achieved through such streamlined and coordinated requirements is proportionate to the increasingly high risks faced including those presenting a cross-border element; they are reasonable and generally corresponding to the interest of the entities involved in ensuring continuity and quality of their services. The costs for ensuring systematic cooperation amongst Member States would be small as compared to the economic and societal losses and damages caused by cybersecurity incidents. Furthermore, the stakeholder consultations held in the context of the review of the NIS Directive, including the results of the Open Public Consultation and targeted surveys, show support for the revision of the NIS Directive along the above-mentioned lines.

- **Choice of the instrument**

The proposal will further streamline the obligations imposed on businesses and ensure a higher level of harmonisation thereof. At the same time, the proposal aims at providing Member States with the flexibility needed to take into account national specificities (such the possibility to identify additional essential or important entities going beyond the baseline set by the legal act). The future legal instrument should therefore be a Directive, as this legal instrument allows for targeted improved harmonisation as well as a certain degree of flexibility for competent authorities.

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

- **Ex-post evaluations/fitness checks of existing legislation**

The Commission has carried out an evaluation of the functioning of the NIS Directive.[5] It has analysed its relevance, EU added value, coherence, effectiveness and efficiency. The main findings of this analysis are:

- The scope of the NIS Directive is too limited in terms of the sectors covered, mainly due to: (i) increased digitisation in recent years and a higher degree of interconnectedness, (ii) the scope of the NIS Directive no longer reflecting all digitised sectors providing key services to the economy and society as a whole.
- The NIS Directive is not sufficiently clear when it comes to the scope for operators of essential services and its provisions do not provide sufficient clarity regarding national competence over digital service providers. This has led to a situation in which certain types of entities have not been identified in all Member States and are therefore not required to put in place security measures and report incidents.
- The NIS Directive allowed wide discretion to the Member States when laying down security and incident reporting requirements for operators of essential services (hereinafter called 'OES(s)'). The evaluation shows that in some instances Member States have implemented these requirements in significantly different ways, creating additional burden for companies operating in more than one Member State.
- The supervision and enforcement regime of the NIS Directive is ineffective. For example, Member States have been very reluctant to apply penalties to entities failing to put in place security requirements or report incidents. This can have negative consequences for the cyber resilience of individual entities.
- The financial and human resources set aside by Member States for fulfilling their tasks (such as OES identification or supervision), and consequently the different levels of maturity in dealing with cybersecurity risks, vary greatly. This further exacerbates the differences in cyber resilience between Member States.
- Member States do not share information systematically with one another, with negative consequences in particular for the effectiveness of the cybersecurity measures and for the level of joint situational awareness at EU level. This is also the case for information sharing among private entities, and for the engagement between the EU level cooperation structures and private entities.

- **Stakeholder consultations**

The Commission has consulted a broad range of stakeholders. Member States and stakeholders were invited to participate in the Open Public Consultation and in the surveys and workshops organised by Wavestone, CEPS and ICF, who the Commission has contracted to carry out a study supporting the review of the NIS Directive. The consulted stakeholders included competent authorities, Union bodies dealing with cybersecurity, operators of essential services, digital service providers, entities providing services outside the scope of the current NIS Directive, trade associations and consumer organisations and citizens.

[5] [Annex 5 of the Impact Assessment]

In addition, the Commission has been in constant touch with the competent authorities in charge of implementing the NIS Directive. The Cooperation Group has extensively covered various cross-cutting and sectoral implementation aspects. Finally, during its NIS country visits in 2019 and 2020, the Commission has interviewed 154 public and private entities, as well as 117 competent authorities.

- **Collection and use of expertise**

The Commission has contracted a consortium of Wavestone, CEPS and ICF to support the Commission in the review of the NIS Directive.[6] The contractor has not only reached out to the stakeholders directly affected by the NIS Directive through target surveys and workshops but has also consulted with a wide range of experts in the field of cybersecurity, such as cybersecurity researchers and cybersecurity industry professionals.

- **Impact assessment**

This proposal is accompanied by an impact assessment[7], which was submitted to the Regulatory Scrutiny Board (RSB) on 23 October 2020 and received a positive opinion with comments by the RSB on 20 November 2020. The RSB recommended improvements in some areas with a view to: (1) better reflect the role of cross-border spillovers in the problem analysis; (2) better explain what success would look like for the initiative; (3) further justify the list of policy options; (4) further elaborate on the costs of the proposed measures. The impact assessment was adjusted to address these points, as well as more detailed comments from the RSB. It now includes more detailed explanations of the role of cross-border spillovers in the field of cybersecurity, a clearer overview of how success can be measured, a more detailed explanation of the design and logic behind the different policy options and actions considered within these options, a more detailed explanation of the aspects analysed in relation to the sectorial scope of the NIS Directive and further clarifications regarding costs.

The Commission considered a number of policy options for improving the legal framework in the area of cyber resilience and incident response:

- "Do nothing": The NIS Directive would remain unchanged and no other measures of non-legislative nature would be taken to target the problems identified by the evaluation of the NIS Directive.
- Option 1: There would be no changes at legislative level. Instead, the Commission would issue recommendations and guidelines (such as on the identification of operators of essential services, security requirements, incident notification procedures and supervision), upon consultation of the Cooperation Group, the EU Agency for Cybersecurity (ENISA) and, as applicable, the network of Computer security incident response teams (CSIRTs).
- Option 2: This option entails targeted amendments to the NIS Directive, including an extension of the scope and several other amendments that would aim at guaranteeing certain immediate solutions to the problems identified, providing more clarity and further harmonisation (such as provisions to harmonise identification thresholds).

[6] Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) – N° 2020-665. Wavestone, CEPS and ICF.

[7] **[Links to final document and to the summary sheet to be added.]**

The amended NIS Directive would however maintain the main building blocks, approach and rationale.

- Option 3: This scenario entails systemic and structural changes to the NIS Directive (through a new directive) envisaging a more fundamental shift of approach towards covering a wider segment of the economies across the Union, yet with a more focused supervision targeting big and key players. It would also streamline the obligations imposed on businesses and ensure a higher level of harmonisation thereof, create a more effective setting for operational aspects, as well as establish a clear basis for enhanced shared responsibilities and accountability of various stakeholders on cybersecurity measures.

The Impact Assessment concludes that the preferred option is option 3 (i.e. systemic and structural changes to the NIS framework). In terms of effectiveness, the preferred option would clearly determine the scope of application of the NIS Directive, extended to a more representative fraction of EU economies and societies, and the streamlining of requirements, along with a more defined framework for supervision and enforcement that would aim at increasing the level of compliance. It also entails measures aimed at improving policy building approaches at Member States level and changing the paradigm thereof, promoting new frameworks for supplier relationships risk management and coordinated vulnerability disclosure. At the same time, the preferred policy option establishes a clear basis for shared responsibilities and accountability and envisages mechanisms aimed at fostering more trust among Member States, both authorities and industry, incentivising information sharing and ensuring a more operational approach, such as the mutual assistance and the peer-review mechanisms. This option would also provide for an EU crisis management framework, building on recently launched EU operational network, and would ensure more involvement of ENISA, within its current mandate, in holding an accurate overview of the cybersecurity state of the Union.

In terms of efficiency, while the preferred option would entail additional compliance and enforcement costs for businesses and Member States, it would also lead to efficient trade-offs and synergies, with the best potential out of all policy options analysed to ensure an increased and consistent level of cyber resilience of key entities across the Union that would eventually lead to cost savings for both businesses and society. This policy option would lead to certain additional administrative burden and compliance costs for the Member States authorities. However, on balance, on the medium and long term it would also bring substantial benefits through increased cooperation among Member States, including at operational level, as well as incentivising, through mutual assistance, peer-review mechanisms and better overview of and interaction with key businesses, an overall increase in cybersecurity capabilities at national and regional level. The preferred policy option would also ensure to a great extent coherence with other legislation, initiatives or policy measures, including sector-specific *lex specialis*.

Addressing the currently persisting insufficiency of cybersecurity preparedness at a Member State level and at the level of companies and other organisations could result in efficiency gains and reduction of additional costs resulting from cybersecurity incidents.

- For essential and important entities, increasing the level of cybersecurity preparedness could result in mitigating potential loss of revenue due to disruptions – including from industrial espionage – and could reduce the large expenses for an ad-hoc threat mitigation. Such gains are likely to outweigh the necessary investment costs. Reducing fragmentation in the internal market would also improve the level playing field among operators.

- For Member States, it could further reduce the risk of growing budgetary expenses for ad-hoc threat mitigation and additional costs in case of emergencies related to cybersecurity incidents.
- For citizens, addressing cybersecurity incidents it is expected to result in reduced loss of income due to economic disruption.

The increased levels of cybersecurity across the Member States and the ability of companies and authorities to respond quickly to an incident and mitigate its impact will most likely result in an increase of the overall trust of citizens in the digital economy, which might have a positive impact on growth and investment.

Increasing the overall level of cybersecurity is likely to lead to an increased overall security and smooth uninterrupted functioning of essential services, which are critical for the society. The initiative may also contribute to other social impacts such as reduced levels of cybercrime and terrorism and increased civil protection. Increasing the level of cyber preparedness for businesses and other organisations may avoid potential financial losses as a result of cyberattacks thus preventing the need to lay off employees.

Increasing the overall level of cybersecurity could also lead to the prevention of environmental risks/damage in case of an attack on an essential service. This could be particularly valid for the energy, water supply and distribution or transport sectors. By strengthening the cybersecurity capabilities, the initiative could lead to more use being made of latest generation ICT infrastructures and services that are also environmentally more sustainable and to the replacement of inefficient and less secure legacy infrastructures. This is expected to contribute also to reducing the number of costly cyber incidents, freeing up resources available for sustainable investments.

- **Regulatory fitness and simplification**

The proposal foresees a general exclusion of micro and small entities from the NIS scope and a lighter *ex-post* supervisory regime applied to a large number of the new entities under the revised scope (so-called important entities). These measures aim to minimise and balance the burden put on companies and public administrations. Furthermore, the proposal replaces the complex identification system for operators of essential services with a generally applicable obligation and introduces a higher level of harmonisation of security and reporting obligations, which would decrease compliance burden, especially for entities providing cross-border services.

The proposal minimizes compliance costs for SMEs, as entities are required to take only those measures necessary to ensure a level of security of network and information systems that is appropriate to the risk presented.

- **Fundamental rights**

The EU is committed to ensuring high standards of protection of fundamental rights. All voluntary information sharing arrangements between entities that this Directive promotes would be conducted in trusted environments in full respect of Union data protection rules, notably Regulation (EU) 2016/679 of the European Parliament and of the Council[8].

[8] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of

4. BUDGETARY IMPLICATIONS

See financial fiche

5. OTHER ELEMENTS

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

The proposal includes a general plan for monitoring and evaluating the impact on the specific objectives, requiring the Commission to carry out a review at least [54 months] after the date of entry into force, and to report to the European Parliament and the Council on its main findings.

The review is to be conducted in line with the Commission's Better Regulation Guidelines.

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

The proposal is structured around several main policy areas, which are inter-related and serve the purpose of raising the level of cybersecurity in the Union.

Subject matter and scope (Article 1 and Article 2)

The Directive, in particular: (a) lays down obligations for the Member States to adopt a national cybersecurity strategy, designate competent national authorities, single points of contact and CSIRTs; (b) provides that Member States shall lay down cybersecurity risk management and reporting obligations for entities referred to as essential entities in Annex I and important entities in Annex II; (c) provides that Member States shall lay down obligations on cybersecurity information sharing.

It applies to certain public or private essential entities operating in the sectors listed in Annex I (energy; transport; banking; financial market infrastructures; health, drinking water; waste water; digital infrastructure; public administration and space) and certain important entities operating in the sectors listed in Annex II (postal and courier services; waste management; manufacture, production and distribution of chemicals; food production, processing and distribution; manufacturing and digital providers). Micro and small entities within the meaning of Commission Recommendation 2003/361/EC of 6 May 2003 are excluded from the scope of the Directive, except for providers of electronic communications networks or of publicly available electronic communications services, trust service providers, Top-level domain name (TLD) name registries and public administration, and certain other entities, such as the sole provider of a service in a Member State.

National cybersecurity frameworks (Articles 5 to 11)

Member States are required to adopt a national cybersecurity strategy defining the strategic objectives and appropriate policy and regulatory measures with a view to achieving and maintaining a high level of cybersecurity.

The Directive also establishes a framework for Coordinated Vulnerability Disclosure and requires Member States to designate CSIRTs to act as trusted intermediaries and facilitate the interaction between the reporting entities and the manufacturers or providers of ICT products

---

such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

and ICT services. ENISA is required to develop and maintain a European vulnerability registry for the discovered vulnerabilities.

Member States are required to put in place National Cybersecurity Crisis Management Frameworks, inter alia by designating national competent authorities responsible for the management of large-scale cybersecurity incidents and crises.

Member States are also required to designate one or more national competent authorities on cybersecurity for the supervisory tasks under this Directive and a national single point of contact on cybersecurity (SPOC) to exercise a liaison function to ensure cross-border cooperation of Member State authorities. Member States are also required to designate CSIRTs.

Cooperation (Articles 12 to 16)

The Directive establishes a Cooperation Group to support and facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence. It also establishes a CSIRTs network to contribute to the development of confidence and trust between the Member States and to promote swift and effective operational cooperation.

A European Cyber Crises Liaison Organisation Network (EU - CyCLONe) is established to support the coordinated management of large-scale cybersecurity incidents and crises and to ensure the regular exchange of information among Member States and EU institutions.

ENISA is required to issue in cooperation with the Commission a biennial report on the state of cybersecurity in the Union.

The Commission is required to establish a peer-review system allowing regular peer-reviews of the Member States' effectiveness of cybersecurity policies.

Cybersecurity risk management and reporting obligations (Articles 17 to 23)

The Directive requires Member States to provide that management bodies of all entities under the scope to approve the cybersecurity risk management measures taken by the respective entities and to follow specific cybersecurity-related training.

Member States are required to ensure that entities under the scope take appropriate and proportionate technical and organisational measures to manage the cybersecurity risks posed to the security of network and information systems. They are also required to ensure that entities notify the national competent authorities or the CSIRTs of any cybersecurity incident having a significant impact on the provision of the service they provide.

TLD registries and the entities providing domain name registration services for the TLD shall collect and maintain accurate and complete domain name registration data. Furthermore, such entities are required to provide efficient access to domain registration data for legitimate access seekers.

Jurisdiction and Registration (Articles 24 and 25)

As a rule, essential and important entities are deemed to be under the jurisdiction of the Member State where they provide their services. However, certain types of entities (DNS service providers, TLD name registries, cloud computing service providers, data centre

service providers and content delivery network providers, as well as certain digital providers) are deemed to be under the jurisdiction of the Member State in which they have their main establishment in the Union. This is to ensure that such entities do not face a multitude of different legal requirements, as they provide services across borders to a particularly high extent. ENISA is required to create and maintain a registry of the later type of entities.

Information sharing (Articles 26 and 27)

Member States shall provide rules enabling entities to engage in cybersecurity-related information sharing within the framework of specific cybersecurity information-sharing arrangements, in compliance with Article 101 TFEU. In addition, Member States shall allow entities outside the scope of this Directive to report, on a voluntary basis, significant incidents, cyber threats or near misses.

Supervision and enforcement (Articles 28 to 34)

Competent authorities are required to supervise the entities under the scope of the Directive, and in particular to ensure their compliance with the security and incident notification requirements. It distinguishes between an ex ante supervisory regime for essential entities and an ex post supervisory regime for important entities, the later requiring competent authorities to take action when provided with evidence or indication that an important entity does not meet the security and incident notification requirements.

The Directive also requires Members States to impose administrative fines to essential and important entities and defines certain maximum fines.

Member States are required to cooperate and assist each other as necessary when entities provide services in more than one Member State or when an entity's main establishment or its representative is located in a certain Member State but its network and information systems are located in one or more other Member States.

2020/0359 (COD)

Proposal for a

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148

(Text with EEA relevance)

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 114 thereof,

Having regard to the proposal from the European Commission,

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

Having regard to the opinion of the European Economic and Social Committee[9],

Having regard to the opinion of the Committee of the Regions[10],

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) Directive (EU) 2016/1148 of the European Parliament and the Council[11] aimed at building cybersecurity capabilities across the Union, mitigating threats to network and information systems used to provide essential services in key sectors and ensuring the continuity of such services when facing cybersecurity incidents, thus contributing to the Union's economy and society to function effectively.

(2) Since the entry into force of Directive (EU) 2016/1148 significant progress has been made in increasing the Union's level of cybersecurity resilience. The review of that Directive has shown that it has served as a catalyst for the institutional and regulatory approach to cybersecurity in the Union, paving the way for a significant change in mind-set. That Directive has ensured the completion of national frameworks by defining national cybersecurity strategies, establishing national capabilities, and implementing regulatory measures covering essential infrastructures and actors identified by each Member State. It has also contributed to cooperation at Union level through the establishment of the Cooperation Group[12] and a network of national Computer Security Incident Response Teams ('CSIRTs network')[13]. Notwithstanding those achievements, the review of Directive (EU) 2016/1148 has revealed inherent

9 OJ C , , p. .

10 OJ C , , p. .

11 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194/1, 19.7.2016 p. 1).

12 Article 11 of Directive (EU) 2016/1148.

13 Article 12 of Directive (EU) 2016/1148.

shortcomings that prevent it from addressing effectively contemporaneous and emerging cybersecurity challenges.

(3) Network and information systems have developed into a central feature of everyday life with the speedy digital transformation and interconnectedness of society, including in cross-border exchanges. That development has led to an expansion of the cybersecurity threat landscape, bringing about new challenges, which require adapted, coordinated and innovative responses in all Member States. The number, magnitude, sophistication, frequency and impact of cybersecurity incidents are increasing, and present a major threat to the functioning of network and information systems. As a result, cyber incidents can impede the pursuit of economic activities in the internal market, generate financial losses, undermine user confidence and cause major damage to the Union economy and society. Cybersecurity preparedness and effectiveness are therefore now more essential than ever to the proper functioning of the internal market.

(4) The legal basis of Directive (EU) 1148/2016 was Article 114 of the Treaty on the Functioning of the European Union (TFEU), the objective of which is the establishment and functioning of the internal market by enhancing measures for the approximation of national rules. The cybersecurity requirements imposed on entities providing services or economically relevant activities vary considerably among Member States in terms of type of requirement, their level of detail and the method of supervision. Those disparities entail additional costs and create difficulties for undertakings that offer goods or services cross-border. Requirements imposed by one Member State that are different from, or even in conflict with, those imposed by another Member State, may substantially affect those cross-border activities. Furthermore, the possibility of suboptimal design or implementation of cybersecurity standards in one Member State is likely to have repercussions on the level of cybersecurity of other Member States, notably given the intense cross-border exchanges. The review of Directive (EU) 2016/1148 has shown a wide divergence in its implementation by Member States, including in relation to its scope, the delimitation of which was very largely left to the discretion of the Member States. Directive (EU) 2016/1148 also provided the Member States with very wide discretion as regards implementing the security and incident reporting obligations set out therein. Those obligations were therefore implemented in significantly different ways at national level. Similar divergence in the implementation occurred in relation to that Directive's provisions on supervision and enforcement.

(5) All those divergences entail a fragmentation of the internal market and are liable to have a prejudicial effect on its functioning, affecting in particular the cross-border provision of services and level of cybersecurity resilience due to the application of different standards. This Directive aims to remove such wide divergences among Member States, in particular by setting out minimum rules regarding the functioning of a coordinated regulatory framework, by laying down mechanisms for the effective cooperation among the responsible authorities in each Member State, by updating the list of sectors and activities subject to cybersecurity obligations and by providing effective remedies and sanctions which are instrumental to the effective enforcement of those obligations. Therefore, Directive (EU) 2016/1148 should be repealed and replaced by this Directive.

(6) This Directive leaves unaffected the ability of Member States to take the necessary measures to ensure the protection of the essential interests of their security, to safeguard public policy and public security, and to allow for the investigation,

detection and prosecution of criminal offences, in compliance with Union law. In accordance with Article 346 TFEU, no Member State is to be obliged to supply information the disclosure of which would be contrary to the essential interests of its public security. In this context, national and Union rules for protecting classified information, non-disclosure agreements, and informal non-disclosure agreements such as the Traffic Light Protocol[14], are of relevance.

(7) With the repeal of Directive (EU) 2016/1148, the scope of application by sectors should be extended to a larger part of the economy in light of the considerations set out in recitals (4) to (6). The sectors covered by Directive (EU) 2016/1148 should therefore be extended to provide a comprehensive coverage of the sectors and services of vital importance for key societal and economic activities within the internal market. The rules should not be different according to whether the entities are operators of essential services or digital service providers. That differentiation has proven obsolete, since it does not reflect the actual importance of the sectors or services for the societal and economic activities in the internal market.

(8) In accordance with Directive (EU) 2016/1148, Member States were responsible for determining which entities meet the criteria to qualify as operators of essential services ('identification process'). In order to eliminate the wide divergences among Member States in that regard and ensure legal certainty for the risk management requirements and reporting obligations for all relevant entities, a uniform criterion should be established that determines the entities falling within the scope of application of this Directive. That criterion should consist of the application of the size-cap rule, whereby all medium and large enterprises, as defined by Commission Recommendation 2003/361/EC[15], that operate within the sectors or provide the type of services covered by this Directive, fall within its scope. Member States should not be required to establish a list of the entities that meet this generally applicable size-related criterion.

(9) However, small or micro entities fulfilling certain criteria that indicate a key role for the economies or societies of Member States or for particular sectors or types of services, should also be covered by this Directive. Member States should be responsible for establishing a list of such entities, and submit it to the Commission.

(10) The Commission, in cooperation with the Cooperation Group, may issue guidelines on the implementation of the criteria applicable to micro and small enterprises.

(11) Depending on the sector in which they operate or the type of service they provide, the entities falling within the scope of this Directive should be classified into two categories: essential and important. That categorisation should take into account the level of criticality of the sector or of the type of service, as well as the level of dependency of other sectors or types of services. Both essential and important entities should be subject to the same risk management requirements and reporting obligations. The supervisory and penalty regimes between these two categories of entities should be differentiated to ensure a fair balance between requirements and obligations on one hand, and the administrative burden stemming from the supervision of compliance on the other hand.

---

14 The Traffic Light Protocol (TLP) is a means for someone sharing information to inform their audience about any limitations in further spreading this information. It is used in almost all CSIRT communities and some Information Analysis and Sharing Centres (ISACs).

15 Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).

(12) Sector-specific legislation and instruments can contribute to ensuring high levels of cybersecurity, while taking full account of the specificities and complexities of those sectors. Where a sector–specific Union legal act requires essential or important entities to adopt cybersecurity risk management measures or to notify incidents or significant cyber threats of at least an equivalent effect to the obligations laid down in this Directive, those sector-specific provisions, including on supervision and enforcement, should apply. The Commission may issue guidelines in relation to the implementation of the *lex specialis*. This Directive does not preclude the adoption of additional sector-specific Union acts addressing cybersecurity risk management measures and incident notifications. This Directive is without prejudice to the existing implementing powers that have been conferred to the Commission in a number of sectors, including transport and energy.

(13) Regulation XXXX/XXXX of the European Parliament and of the Council[16] should be considered to be a sector-specific Union legal act in relation to this Directive with regard to the financial sector entities. The provisions of Regulation XXXX/XXXX relating to information and communications technology (ICT) risk management measures, management of ICT-related incidents and notably incident reporting, as well as on digital operational resilience testing, information sharing arrangements and ICT third party risk should apply instead of those set up under this Directive. Member States should therefore not apply the provisions of this Directive on cybersecurity risk management and reporting obligations, information sharing and supervision and enforcement to any financial entities covered by Regulation XXXX/XXXX. At the same time, it is important to maintain a strong relationship and the exchange of information with the financial sector under this Directive. To that end, Regulation XXXX/XXXX allows all financial supervisors, the European Supervisory Authorities (ESAs) for the financial sector and the national competent authorities under Regulation XXXX/XXXX, to participate in strategic policy discussions and technical workings of the Cooperation Group, and to exchange information and cooperate with the single points of contact designated under this Directive and with the national CSIRTs. The competent authorities under Regulation XXXX/XXXX should transmit details of major ICT-related incidents also to the single points of contact designated under this Directive. Moreover, Member States should continue to include the financial sector in their cybersecurity strategies and national CSIRTs may cover the financial sector in their activities.

(14) In view of the interlinkages between cybersecurity and the physical security of entities, a coherent approach should be ensured between Directive (EU) XXX/XXX of the European Parliament and of the Council[17] and this Directive. To achieve this, Member States should ensure that critical entities, and equivalent entities, pursuant to Directive (EU) XXX/XXX are considered to be essential entities under this Directive. Member States should also ensure that their cybersecurity strategies provide for a policy framework for enhanced coordination between the competent authority under this Directive and the one under Directive (EU) XXX/XXX in the context of information sharing on incidents and cyber threats and the exercise of supervisory tasks. Authorities under both Directives should cooperate and exchange information, particularly in relation to the identification of critical entities, cyber threats, cybersecurity risks, incidents affecting critical entities as well as on the cybersecurity

16 *[insert the full title and OJ publication reference when known]*
17 *[insert the full title and OJ publication reference when known]*

measures taken by critical entities. Upon request of competent authorities under Directive (EU) XXX/XXX, competent authorities under this Directive should be allowed to exercise their supervisory and enforcement powers on an essential entity identified as critical. Both authorities should cooperate and exchange information for this purpose.

(15) Upholding and preserving a reliable, resilient and secure domain name system (DNS) is a key factor in maintaining the integrity of the Internet and is essential for its continuous and stable operation, on which the digital economy and society depend. Therefore, this Directive should apply to all providers of DNS services along the DNS resolution chain, including operators of root name servers, top-level-domain (TLD) name servers, authoritative name servers for domain names and recursive resolvers.

(16) Cloud computing services should cover services that allow on-demand and broad remote access to a scalable and elastic pool of shareable and distributed computing resources. Those computing resources include resources such as networks, servers or other infrastructure, operating systems, software, storage, applications and services. The deployment models of cloud computing should include private, community, public and hybrid cloud. The aforementioned service and deployment models have the same meaning as the terms of service and deployment models defined under ISO/IEC 17788:2014 standard. The capability of the cloud computing user to unilaterally self-provision computing capabilities, such as server time or network storage, without any human interaction by the cloud computing service provider could be described as on-demand administration. The term 'broad remote access' is used to describe that the cloud capabilities are provided over the network and accessed through mechanisms promoting use of heterogeneous thin or thick client platforms (including mobile phones, tablets, laptops, workstations). The term 'scalable' refers to computing resources that are flexibly allocated by the cloud service provider, irrespective of the geographical location of the resources, in order to handle fluctuations in demand. The term 'elastic pool' is used to describe those computing resources that are provisioned and released according to demand in order to rapidly increase and decrease resources available depending on workload. The term 'shareable' is used to describe those computing resources that are provided to multiple users who share a common access to the service, but where the processing is carried out separately for each user, although the service is provided from the same electronic equipment. The term 'distributed' is used to describe those computing resources that are located on different networked computers or devices and which communicate and coordinate among themselves by message passing.

(17) Given the emergence of innovative technologies and new business models, new cloud computing deployment and service models are expected to appear on the market in response to evolving customer needs. In that context, cloud computing services may be delivered in a highly distributed form, even closer to where data are being generated or collected, thus moving from the traditional model to a highly distributed one ('edge computing').

(18) Services offered by data centre service providers may not always be provided in a form of cloud computing service. Accordingly, data centres may not always constitute a part of cloud computing infrastructure. In order to manage all the risks posed to the security of network and information systems, this Directive should cover also providers of such data centre services that are not cloud computing services. For the purpose of this Directive, the term 'data centre service' should cover provision of a service that encompasses structures, or groups of structures, dedicated to the

centralised accommodation, interconnection and operation of information technology and network equipment providing data storage, processing and transport services together with all the facilities and infrastructures for power distribution and environmental control. The term 'data centre service' does not apply to in-house, corporate data centres owned and operated for own purposes of the concerned entity.

(19) Postal service providers within the meaning of Directive 97/67/EC of the European Parliament and of the Council[18], as well as express and courier delivery service providers, should be subject to this Directive if they provide at least one of the steps in the postal delivery chain and in particular clearance, sorting or distribution, including pick-up services. Transport services that are not undertaken in conjunction with one of those steps should fall outside of the scope of postal services.

(20) Those growing interdependencies are the result of an increasingly cross-border and interdependent network of service provision using key infrastructures across the Union in the sectors of energy, transport, digital infrastructure, drinking and waste water, health, certain aspects of public administration, as well as space in as far as the provision of certain services depending on ground-based infrastructures that are owned, managed and operated either by Member States or by private parties is concerned, therefore not covering infrastructures owned, managed or operated by or on behalf of the Union as part of its space programmes. Those interdependencies mean that any disruption, even one initially confined to one entity or one sector, can have cascading effects more broadly, potentially resulting in far-reaching and long-lasting negative impacts in the delivery of services across the internal market. The COVID-19 pandemic has shown the vulnerability of our increasingly interdependent societies in the face of low-probability risks.

(21) In view of the differences in national governance structures and in order to safeguard already existing sectoral arrangements or Union supervisory and regulatory bodies, Member States should be able to designate more than one national competent authority responsible for fulfilling the tasks linked to the security of the network and information systems of essential and important entities under this Directive. Member States should be able to assign this role to an existing authority.

(22) In order to facilitate cross-border cooperation and communication among authorities and to enable this Directive to be implemented effectively, it is necessary for each Member State to designate a national single point of contact responsible for coordinating issues related to the security of network and information systems and cross-border cooperation at Union level.

(23) Competent authorities or the CSIRTs should receive notifications of incidents from entities in an effective and efficient way. The single points of contact should be tasked with forwarding incident notifications to the single points of contact of other affected Member States. At the level of Member States' authorities, to ensure one single entry point in every Member States, the single points of contacts should also be the addressees of relevant information on incidents concerning financial sector entities from the competent authorities under Regulation XXXX/XXXX which they should be able to forward, as appropriate, to the relevant national competent authorities or CSIRTs under this Directive.

---

[18] Directive 97/67/EC of the European Parliament and of the Council of 15 December 1997 on common rules for the development of the internal market of Community postal services and the improvement of quality of service (OJ L 15, 21.1.1998, p. 14).

(24) Member States should be adequately equipped, in terms of both technical and organisational capabilities, to prevent, detect, respond to and mitigate network and information system incidents and risks. Member States should therefore ensure that they have well-functioning CSIRTs, also known as computer emergency response teams ('CERTs'), complying with essential requirements in order to guarantee effective and compatible capabilities to deal with incidents and risks and to ensure efficient cooperation at Union level. In view of enhancing the trust relationship between the entities and the CSIRTs, in cases where a CSIRT is part of the competent authority, Member States should consider functional separation between the operational tasks provided by CSIRTs, notably in relation to information sharing and support to the entities, and the supervisory activities of competent authorities.

(25) As regards personal data, CSIRTs should be able to provide, in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council[19] as regards personal data, on behalf of and upon request by an entity under this Directive, a proactive scanning of the network and information systems used for the provision of their services. Member States should aim at ensuring an equal level of technical capabilities for all sectorial CSIRTs. Member States may request the assistance of the European Union Agency for Cybersecurity (ENISA) in developing national CSIRTs.

(26) Given the importance of international cooperation on cybersecurity, CSIRTs should be able to participate in international cooperation networks in addition to the CSIRTs network established by this Directive.

(27) In accordance with the Annex to Commission Recommendation (EU) 2017/1548 on Coordinated Response to Large Scale Cybersecurity Incidents and Crises ('Blueprint')[20], a large-scale incident should mean an incident with a significant impact on at least two Member States or whose disruption exceeds a Member State's capacity to respond to it. Depending on their cause and impact, large-scale incidents may escalate and turn into fully-fledged crises not allowing the proper functioning of the internal market. Given the wide-ranging scope and, in most cases, the cross-border nature of such incidents, Member States and relevant Union institutions, bodies and agencies should cooperate at technical, operational and political level to properly coordinate the response across the Union.

(28) Since the exploitation of vulnerabilities in network and information systems may cause significant disruption and harm, swiftly identifying and remedying those vulnerabilities is an important factor in reducing cybersecurity risk. Entities that develop such systems should therefore establish appropriate procedures to handle vulnerabilities when they are discovered. Since vulnerabilities are often discovered and reported (disclosed) by third parties (reporting entities), the manufacturer or provider of ICT products or services should also put in place the necessary procedures to receive vulnerability information from third parties. In this regard, international standards ISO/IEC 30111 and ISO/IEC 29417 provide guidance on vulnerability handling and vulnerability disclosure respectively. As regards vulnerability disclosure, coordination between reporting entities and manufacturers or providers of ICT

---

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

20 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).

products or services is particularly important. Coordinated vulnerability disclosure specifies a structured process through which vulnerabilities are reported to organisations in a manner allowing the organisation to diagnose and remedy the vulnerability before detailed vulnerability information is disclosed to third parties or to the public. Coordinated vulnerability disclosure should also comprise coordination between the reporting entity and the organisation as regards the timing of remediation and publication of vulnerabilities.

(29) Member States should therefore take measures to facilitate coordinated vulnerability disclosure by establishing a relevant national policy. In this regard, Member States should designate a CSIRT to take the role of 'coordinator', acting as an intermediary between the reporting entities and the manufacturers or providers of ICT products or services where necessary. The tasks of the CSIRT coordinator should in particular include identifying and contacting concerned entities, supporting reporting entities, negotiating disclosure timelines, and managing vulnerabilities that affect multiple organisations (multi-party vulnerability disclosure). Where vulnerabilities affect multiple manufacturers or providers of ICT products or services established in more than one Member State, the designated CSIRTs from each of the affected Member States should cooperate within the CSIRTs Network.

(30) Access to correct and timely information on vulnerabilities affecting ICT products and services contributes to an enhanced cybersecurity risk management. In that regard, sources of publicly available information on vulnerabilities are an important tool for entities and their users, but also national competent authorities and CSIRTs. For this reason, ENISA should establish a vulnerability registry where, essential and important entities and their suppliers, as well as entities which do not fall in the scope of application of this Directive may, on a voluntary basis, disclose vulnerabilities and provide the vulnerability information that allows users to take appropriate mitigating measures.

(31) Although similar vulnerability registries or databases do exist, these are hosted and maintained by entities which are not established in the Union. A European vulnerability registry maintained by ENISA would provide improved transparency regarding the publication process before the vulnerability is officially disclosed, and resilience in cases of disruptions or interruptions on the provision of similar services. To avoid duplication of efforts and seek complementarity to the extent possible, ENISA should explore the possibility of entering into structured cooperation agreements with similar registries in third country jurisdictions.

(32) The Cooperation Group should establish a work programme every two years including the actions to be undertaken by the Group to implement its objectives and tasks. The timeframe of the first programme adopted under this Directive should be aligned with the timeframe of the last programme adopted under Directive (EU) 2016/1148 in order to avoid potential disruptions in the work of the Group.

(33) When developing guidance documents, the Cooperation Group should consistently: map national solutions and experiences, assess the impact of Cooperation Group deliverables on national approaches, discuss implementation challenges and formulate specific recommendations to be addressed through better implementation of existing rules.

(34) The Cooperation Group should remain a flexible forum and be able to react to changing and new policy priorities and challenges while taking into account the availability of resources. It should organize regular joint meetings with relevant

private stakeholders from across the Union to discuss activities carried out by the Group and gather input on emerging policy challenges. In order to enhance cooperation at Union level, the Group should consider inviting Union bodies and agencies involved in cybersecurity policy, such as the European Cybercrime Centre (EC3), the European Union Aviation Safety Agency (EASA) and the European Union Agency for Space Programme (EUSPA) to participate in its work.

(35) The competent authorities and CSIRTs should be empowered to participate in exchange schemes for officials from other Member States in order to improve cooperation. The competent authorities should take the necessary measures to enable officials from other Member States to play an effective role in the activities of the host competent authority.

(36) The Union should, where appropriate, conclude international agreements, in accordance with Article 218 TFEU, with third countries or international organisations, allowing and organising their participation in some activities of the Cooperation Group and the CSIRTs network. Such agreements should ensure adequate protection of data.

(37) Member States should contribute to the establishment of the EU Cybersecurity Crisis Response Framework set out in Recommendation (EU) 2017/1584 through the existing cooperation networks, notably the Cyber Crisis Liaison Organisation Network (EU-CyCLONe), CSIRTs network and the Cooperation Group. EU-CyCLONe and the CSIRTs network should cooperate on the basis of procedural arrangements defining the modalities of that cooperation. The EU-CyCLONe's rules of procedures should further specify the modalities through which the network should function, including but not limited to roles, cooperation modes, interactions with other relevant actors and templates for information sharing, as well as means of communication. For crisis management at Union level, relevant parties should rely on the Integrated Political Crisis Response (IPCR) arrangements. The Commission should use the ARGUS high-level cross-sectoral crisis coordination process for this purpose. If the crisis entails an important external or Common Security and Defence Policy (CSDP) dimension, the European External Action Service (EEAS) Crisis Response Mechanism (CRM) should be activated.

(38) For the purposes of this Directive, the term 'risk' should refer to the potential for loss or disruption caused by a cybersecurity incident and should be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of said incident.

(39) For the purposes of this Directive, the term 'near misses' should refer to an event which could potentially have caused harm, but was successfully prevented from fully transpiring.

(40) Risk-management measures should include measures to identify any risks of incidents, to prevent, detect and handle incidents and to mitigate their impact. The security of network and information systems should comprise the security of stored, transmitted and processed data.

(41) In order to avoid imposing a disproportionate financial and administrative burden on essential and important entities, the cybersecurity risk management requirements should be proportionate to the risk presented by the network and information system concerned, taking into account the state of the art of such measures.

(42) Essential and important entities should ensure the security of the network and information systems which they use in their activities. Those are primarily private network and information systems managed by their internal IT staff or the security of which has been outsourced. The cybersecurity risk management and reporting requirements pursuant to this Directive should apply to the relevant essential and important entities regardless of whether they perform the maintenance of their network and information systems internally or outsource it.

(43) Addressing cybersecurity risks stemming from an entity's supply chain and its relationship with its suppliers is particularly important given the prevalence of incidents where entities have fallen victim to cyber-attacks and where malicious actors were able to compromise the security of an entity's network and information systems by exploiting vulnerabilities affecting third party products and services. Entities should therefore assess and take into account the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures.

(44) Among service providers, managed security services providers (MSSPs) in areas such as incident response, penetration testing, security audits and consultancy play a particularly important role in assisting entities in their efforts to detect and respond to incidents. Those MSSPs have however also been the targets of cyberattacks themselves and through their close integration in the operations of operators pose a particular cybersecurity risk. Entities should therefore exercise increased diligence in selecting an MSSP.

(45) Entities should also address cybersecurity risks stemming from their interactions and relationships with other stakeholders within a broader ecosystem. In particular, entities should take appropriate measures to ensure that their cooperation with academic and research institutions takes place in line with their cybersecurity policies and follows good practices as regards secure access and dissemination of information in general and the protection of intellectual property in particular. Similarly, given the importance and value of data for the activities of the entities, when relying on data transformation and data analytics services from third parties, the entities should take all appropriate cybersecurity measures.

(46) To further address key supply chain risks and assist entities operating in sectors covered by this Directive to appropriately manage supply chain and supplier related cybersecurity risks, the Cooperation Group involving relevant national authorities, in cooperation with the Commission and ENISA, should carry out coordinated sectoral supply chain risk assessments, as was already done for 5G networks following Recommendation (EU) 2019/534 on Cybersecurity of 5G networks[21], with the aim of identifying per sector which are the critical ICT services, systems or products, relevant threats and vulnerabilities.

(47) The supply chain risk assessments, in light of the features of the sector concerned, should take into account both technical and, where relevant, non-technical factors including those defined in Recommendation (EU) 2019/534, in the EU wide coordinated risk assessment of 5G networks security and in the EU Toolbox on 5G cybersecurity agreed by the Cooperation Group. To identify the supply chains that should be subject to a coordinated risk assessment, the following criteria should be

[21] Commission Recommendation (EU) 2019/534 of 26 March 2019 Cybersecurity of 5G networks (OJ L 88, 29.3.2019, p. 42).

taken into account: (i) the extent to which essential and important entities use and rely on specific critical ICT services, systems or products; (ii) the relevance of specific critical ICT services, systems or products for performing critical or sensitive functions, including the processing of personal data; (iii) the availability of alternative ICT services, systems or products; (iv) the resilience of the overall supply chain of ICT services, systems or products against disruptive events and (v) for emerging ICT services, systems or products, their potential future significance for the entities' activities.

(48) In order to streamline the legal obligations imposed on providers of public electronic communications networks or publicly available electronic communications services, and trust service providers related to the security of their network and information systems, as well as to enable those entities and their respective competent authorities to benefit from the legal framework established by this Directive (including designation of CSIRT responsible for risk and incident handling, participation of competent authorities and bodies in the work of the Cooperation Group and the CSIRT network), they should be included in the scope of application of this Directive. The corresponding provisions laid down in Regulation (EU) No 910/2014 of the European Parliament and of the Council[22] and Directive (EU) 2018/1972 of the European Parliament and of the Council[23] related to the imposition of security and notification requirement on these types of entities should therefore be repealed. The rules on reporting obligations should be without prejudice to Regulation (EU) 2016/679 and Directive 2002/58/EC of the European Parliament and of the Council[24].

(49) Where appropriate and to avoid unnecessary disruption, existing national guidelines and national legislation adopted for the transposition of the rules related to security measures laid down in Article 40(1) of Directive (EU) 2018/1972, as well as of the requirements of Article 40(2) of that Directive concerning the parameters related to the significance of an incident, should continue to be used by the competent authorities in charge of supervision and enforcement for the purposes of this Directive.

(50) Given the growing importance of number-independent interpersonal communications services, it is necessary to ensure that such services are also subject to appropriate security requirements in view of their specific nature and economic importance. Providers of such services should thus also ensure a level of security of network and information systems appropriate to the risk posed. Given that providers of number-independent interpersonal communications services normally do not exercise actual control over the transmission of signals over networks, the degree of risk for such services can be considered in some respects to be lower than for traditional electronic communications services. The same applies to interpersonal communications services which make use of numbers and which do not exercise actual control over signal transmission.

---

22 Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73).

23 Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (OJ L 321, 17.12.2018, p. 36).

24 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

(51) The internal market is more reliant on the functioning of the internet than ever before. The services of virtually all essential and important entities are dependent on services provided over the internet. In order to ensure the smooth provision of services provided by essential and important entities, it is important that public electronic communications networks, such as, for example, internet backbones or submarine communications cables, have appropriate cybersecurity measures in place and report incidents in relation thereto.

(52) Where appropriate, entities should inform their service recipients of particular and significant threats and of measures they can take to mitigate the resulting risk to themselves. The requirement to inform those recipients of such threats should not discharge entities from the obligation to take, at their own expense, appropriate and immediate measures to prevent or remedy any cyber threats and restore the normal security level of the service. The provision of such information about security threats to the recipients should be free of charge.

(53) In particular, providers of public electronic communications networks or publicly available electronic communications services, should inform the service recipients of particular and significant cyber threats and of measures they can take to protect the security of their communications, for instance by using specific types of software or encryption technologies.

(54) In order to safeguard the security of electronic communications networks and services, the use of encryption, and in particular end-to-end encryption, should be promoted and, where necessary, should be mandatory for providers of such services and networks in accordance with the principles of security and privacy by default and by design for the purposes of Article 18. The use of end-to-end encryption should be reconciled with the Member State' powers to ensure the protection of their essential security interests and public security, and to permit the investigation, detection and prosecution of criminal offences in compliance with Union law. Solutions for lawful access to information in end-to-end encrypted communications should maintain the effectiveness of encryption in protecting privacy and security of communications, while providing an effective response to crime.

(55) This Directive lays down a two-stage approach to incident reporting in order to strike the right balance between, on the one hand, swift reporting that helps mitigate the potential spread of incidents and allows entities to seek support, and, on the other hand, in-depth reporting that draws valuable lessons from individual incidents and improves over time the resilience to cyber threats of individual companies and entire sectors. Where entities become aware of an incident, they should be required to submit an initial notification within 24 hours, followed by a final report not later than one month after. The initial notification should only include the information strictly necessary to make the competent authorities aware of the incident and allow the entity to seek assistance, if required. Such notification, where applicable, should indicate whether the incident is presumably caused by unlawful or malicious action. Member States should ensure that the requirement to submit this initial notification does not divert the reporting entity's resources from activities related to incident handling that should be prioritised. To further prevent that incident reporting obligations either divert resources from incident response handling or may otherwise compromise the entities efforts in that respect, Member States should also provide that, in duly justified cases and in agreement with the competent authorities or the CSIRT, the entity concerned can deviate from the deadlines of 24 hours for the initial notification and one month for the final report.

(56) Essential and important entities are often in a situation where a particular incident, because of its features, needs to be reported to various authorities as a result of notification obligations included in various legal instruments. Such cases create additional burdens and may also lead to uncertainties with regard to the format and procedures of such notifications. In view of this and, for the purposes of simplifying the reporting of security incidents, Member States should establish *a single entry point* for all notifications required under this Directive and also under other Union law such as Regulation (EU) 2016/679 and Directive 2002/58/EC. ENISA, in cooperation with the Cooperation Group should develop common notification templates by means of guidelines that would simplify and streamline the reporting information requested by Union law and decrease the burdens for companies.

(57) Where it is suspected that an incident is related to serious criminal activities under Union or national law, Member States should encourage essential and important entities, on the basis of applicable criminal proceedings rules in compliance with Union law, to report incidents of a suspected serious criminal nature to the relevant law enforcement authorities. Where appropriate, and without prejudice to the personal data protection rules applying to Europol, it is desirable that coordination between competent authorities and law enforcement authorities of different Member States be facilitated by the EC3 and ENISA.

(58) Personal data are in many cases compromised as a result of incidents. In this context, competent authorities should cooperate and exchange information on all relevant matters with data protection authorities and the supervisory authorities pursuant to Directive 2002/58/EC.

(59) Maintaining accurate and complete databases of domain names and registration data (so called 'WHOIS data') and providing lawful access to such data is essential to ensure the security, stability and resilience of the DNS, which in turn contributes to a high common level of cybersecurity within the Union. Where processing includes personal data such processing shall comply with Union data protection law.

(60) The availability and timely accessibility of these data to public authorities, including competent authorities under Union or national law for the prevention, investigation or prosecution of criminal offences, CERTs, (CSIRTs, and as regards the data of their clients to providers of electronic communications networks and services and providers of cybersecurity technologies and services acting on behalf of those clients, is essential to prevent and combat Domain Name System abuse, in particular to prevent, detect and respond to cybersecurity incidents. Such access should comply with Union data protection law insofar as it is related to personal data.

(61) In order to ensure the availability of accurate and complete domain name registration data, TLD registries and the entities providing domain name registration services for the TLD (so-called registrars) should collect and guarantee the integrity and availability of domain names registration data. In particular, TLD registries and the entities providing domain name registration services for the TLD should establish policies and procedures to collect and maintain accurate and complete registration data, as well as to prevent and correct inaccurate registration data in accordance with Union data protection rules.

(62) TLD registries and the entities providing domain name registration services for them should make publically available domain name registration data that fall outside the

scope of Union data protection rules, such as data that concern legal persons[25]. TLD registries and the entities providing domain name registration services for the TLD should also enable lawful access to specific domain name registration data concerning natural persons to legitimate access seekers, in accordance with Union data protection law. Member States should ensure that TLD registries and the entities providing domain name registration services for them should respond without undue delay to requests from legitimate access seekers for the disclosure of domain name registration data. TLD registries and the entities providing domain name registration services for them should establish policies and procedures for the publication and disclosure of registration data, including service level agreements to deal with requests for access from legitimate access seekers. The access procedure may also include the use of an interface, portal or other technical tool to provide an efficient system for requesting and accessing registration data. With a view to promoting harmonised practices across the internal market, the Commission may adopt guidelines on such procedures without prejudice to the competences of the European Data Protection Board.

(63) All essential and important entities under this Directive should fall under the jurisdiction of the Member State where they provide their services. If the entity provides services in more than one Member State, it should fall under the separate and concurrent jurisdiction of each of these Member States. The competent authorities of these Member States should cooperate, provide mutual assistance to each other and where appropriate, carry out joint supervisory actions.

(64) In order to take account of the cross-border nature of the services and operations of DNS service providers, TLD name registries, content delivery network providers, cloud computing service providers, data centre service providers and digital providers, only one Member State should have jurisdiction over these entities. Jurisdiction should be attributed to the Member State in which the respective entity has its main establishment in the Union. The criterion of establishment for the purposes of this Directive implies the effective exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect. Whether this criterion is fulfilled should not depend on whether the network and information systems are physically located in a given place; the presence and use of such systems do not, in themselves, constitute such main establishment and are therefore not decisive criteria for determining the main establishment. The main establishment should be the place where the decisions related to the cybersecurity risk management measures are taken in the Union. This will typically correspond to the place of the companies' central administration in the Union. If such decisions are not taken in the Union, the main establishment should be deemed to be in the Member States where the entity has an establishment with the highest number of employees in the Union. Where the services are carried out by a group of undertakings, the main establishment of the controlling undertaking should be considered to be the main establishment of the group of undertakings.

(65) In cases where a DNS service provider, TLD name registry, content delivery network provider, cloud computing service provider, data centre service provider and digital

[25] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL recital (14) whereby "this Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person".

provider not established in the Union offers services within the Union, it should designate a representative. In order to determine whether such an entity is offering services within the Union, it should be ascertained whether it is apparent that the entity is planning to offer services to persons in one or more Member States. The mere accessibility in the Union of the entity's or an intermediary's website or of an email address and of other contact details, or the use of a language generally used in the third country where the entity is established, is as such insufficient to ascertain such an intention. However, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the entity is planning to offer services within the Union. The representative should act on behalf of the entity and it should be possible for competent authorities or the CSIRTs to contact the representative. The representative should be explicitly designated by a written mandate of the entity to act on the latter's behalf with regard to the latter's obligations under this Directive, including incident reporting.

(66) Where information considered classified according to national or Union law is exchanged, reported or otherwise shared under the provisions of this Directive, the corresponding specific rules on the handling of classified information should be applied.

(67) With cyber threats becoming more complex and sophisticated, good detection and prevention measures depend to a large extent on regular threat and vulnerability intelligence sharing between entities. Information sharing contributes to increased awareness on cyber threats, which, in turn, enhances the entities' capacity to prevent threats from materialising into real incidents and enables the entities to better contain the effects of incidents and recover more efficiently. In the absence of guidance at Union level, several factors seem to have inhibited such intelligence sharing, notably uncertainty over the compatibility with competition and liability rules.

(68) Entities should be encouraged to collectively leverage their individual knowledge and practical experience at strategic, tactical and operational levels with a view to enhance their capabilities to adequately assess, monitor, defend against, and respond to, cyber threats. It is thus necessary to enable the emergence at Union level of mechanisms for voluntary information sharing arrangements. To this end, Member States should actively support and encourage also relevant entities not covered by the scope of this Directive to participate in such information-sharing mechanisms. Those mechanisms should be conducted in full compliance with the competition rules of the Union as well as the data protection Union law rules.

(69) The processing of personal data, to the extent strictly necessary and proportionate for the purposes of ensuring network and information security by entities, public authorities, CERTs, CSIRTs, and providers of security technologies and services should constitute a legitimate interest of the data controller concerned, as referred to in Regulation (EU) 2016/679. That should include measures related to the prevention, detection, analysis and response to incidents, measures to raise awareness in relation to specific cyber threats, exchange of information in the context of vulnerability remediation and coordinated disclosure, as well as the voluntary exchange of information on those incidents, as well as cyber threats and vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools. Such measures may require the processing of the following types

of personal data: IP addresses, uniform resources locators (URLs), domain names, and email addresses.

(70) In order to strengthen the supervisory powers and actions that help ensure effective compliance, this Directive should provide for a minimum list of supervisory actions and means through which competent authorities may supervise essential and important entities. In addition, this Directive should establish a differentiation of supervisory regime between essential and important entities with a view to ensuring a fair balance of obligations for both entities and competent authorities. Thus, essential entities should be subject to a fully-fledged supervisory regime (*ex-ante* and *ex-post*), while important entities should be subject to a light supervisory regime, *ex-post* only. For the latter, this means that important entities should not document systematically compliance with cybersecurity risk management requirements, while competent authorities should implement a reactive *ex -post* approach to supervision and, hence, not have a general obligation to supervise those entities.

(71) In order to make enforcement effective, a minimum list of administrative sanctions for breach of the cybersecurity risk management and reporting obligations provided by this Directive should be laid down, setting up a clear and consistent framework for such sanctions across the Union. Due regard should be given to the nature, gravity and duration of the infringement, the actual damage caused or losses incurred or potential damage or losses that could have been triggered, the intentional or negligent character of the infringement, actions taken to prevent or mitigate the damage and/or losses suffered, the degree of responsibility or any relevant previous infringements, the degree of cooperation with the competent authority and any other aggravating or mitigating factor. The imposition of penalties including administrative fines should be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter of Fundamental Rights of the European Union, including effective judicial protection and due process.

(72) In order to ensure effective enforcement of the obligations laid down in this Directive, each competent authority should have the power to impose or request the imposition of administrative fines.

(73) Where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes. Where administrative fines are imposed on persons that are not an undertaking, the supervisory authority should take account of the general level of income in the Member State as well as the economic situation of the person in considering the appropriate amount of the fine. It should be for the Member States to determine whether and to what extent public authorities should be subject to administrative fines. Imposing an administrative fine does not affect the application of other powers by the competent authorities or of other penalties laid down in the national rules transposing this Directive.

(74) Member States should be able to lay down the rules on criminal penalties for infringements of the national rules transposing this Directive. However, the imposition of criminal penalties for infringements of such national rules and of related administrative penalties should not lead to a breach of the principle of *ne bis in idem*, as interpreted by the Court of Justice.

(75) Where this Directive does not harmonise administrative penalties or where necessary in other cases, for example in cases of serious infringements of the obligations laid down in this Directive, Member States should implement a system which provides for

effective, proportionate and dissuasive penalties. The nature of such penalties, criminal or administrative, should be determined by Member State law.

(76) In order to further strengthen the effectiveness and dissuasiveness of the penalties applicable to infringements of obligations laid down pursuant to this Directive, the competent authorities should be empowered to apply sanctions consisting of the suspension of a certification or authorisation concerning part or all the services provided by an essential entity and the imposition of a temporary ban from the exercise of managerial functions by a natural person. Given their severity and impact on the entities' activities and ultimately on their consumers, such sanctions should only be applied proportionally to the severity of the infringement and taking account of the specific circumstances of each case, including the intentional or negligent character of the infringement, actions taken to prevent or mitigate the damage and/or losses suffered. Such sanctions should only be applied as ultima ratio, meaning only after the other relevant enforcement actions laid down by this Directive have been exhausted, and only for the time until the entities to which they apply take the necessary action to remedy the deficiencies or comply with the requirements of the competent authority for which such sanctions were applied. The imposition of such sanctions shall be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter of Fundamental Rights of the European Union, including effective judicial protection, due process, presumption of innocence and right of defence.

(77) This Directive should establish cooperation rules between the competent authorities and the supervisory authorities in accordance with Regulation (EU) 2016/679 to deal with infringements related to personal data.

(78) This Directive should aim at ensuring a high level of responsibility for the cybersecurity risk management measures and reporting obligations at the level of the organisations. For these reasons, the management bodies of the entities falling within the scope of this Directive should approve the cybersecurity risk measures and supervise their implementation.

(79) A peer-review mechanism should be introduced, allowing the assessment by experts designated by the Member States of the implementation of cybersecurity policies, including the level of Member States' capabilities and available resources.

(80) In order to take into account new cyber threats, technological developments or sectorial specificities, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission in respect of the elements in relation to risk management measures required by this Directive. The Commission should also be empowered to adopt delegated acts establishing which categories of essential entities shall be required to obtain a certificate and under which specific European cybersecurity certification schemes. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Inter-institutional Agreement of 13 April 2016 on Better Law-Making[26]. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

[26] OJ L 123, 12.5.2016, p. 1.

(81) In order to ensure uniform conditions for the implementation of the relevant provisions of this Directive concerning the procedural arrangements necessary for the functioning of the Cooperation Group, the technical elements related to risk management measures or the type of information, the format and the procedure of incident notifications, implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council.[27]

(82) The Commission should periodically review this Directive, in consultation with interested parties, in particular with a view to determining the need for modification in the light of changes to societal, political, technological or market conditions.

(83) Since the objective of this Directive, namely to achieve a high common level of cybersecurity in the Union, cannot be sufficiently achieved by the Member States but can rather, by reason of the effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Directive does not go beyond what is necessary in order to achieve that objective.

(84) This Directive respects the fundamental rights, and observes the principles, recognised by the Charter of Fundamental Rights of the European Union, in particular the right to respect for private life and communications, the protection of personal data, the freedom to conduct a business, the right to property, the right to an effective remedy before a court and the right to be heard. This Directive should be implemented in accordance with those rights and principles,

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I

General provisions

Article 1

Subject matter

1. This Directive lays down measures with a view to ensuring a high common level of cybersecurity within the Union.

2. To that end, this Directive:

(a) lays down obligations on Member States to adopt national cybersecurity strategies, designate competent national authorities, single points of contact and computer security incident response teams (CSIRTs);

(b) lays down cybersecurity risk management and reporting obligations for entities of a type referred to as essential entities in Annex I and important entities in Annex II;

[27] Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

(c) lays down obligations on cybersecurity information sharing.

Article 2

Scope

1. This Directive applies to public and private entities of a type referred to as essential entities in Annex I and as important entities in Annex II. This Directive does not apply to entities that qualify as micro and small enterprises within the meaning of Commission Recommendation 2003/361/EC.[28]

2. However, regardless of their size, this Directive also applies to entities referred to in Annexes I and II, where:

   (a) the services are provided by one of the following entities:

      (i) public electronic communications networks or publicly available electronic communications services referred to in point 8 of Annex I;

      (ii) trust service providers referred to point 8 of Annex I;

      (iii) top–level domain name registries and domain name system (DNS) service providers referred to in point 8 of Annex I;

   (b) the entity is a public administration entity as defined in point 23 of Article 4;

   (c) the entity is the sole provider of a service in a Member State;

   (d) a potential disruption of the service provided by the entity could have an impact on public safety, public security or public health;

   (e) a potential disruption of the service provided by the entity could induce systemic risks, in particular for the sectors where such disruption could have a cross-border impact;

   (f) the entity is critical because of its specific importance at regional or national level for the particular sector or type of service, or for other interdependent sectors in the Member State;

   (g) the entity is identified as a critical entity pursuant to Directive (EU) XXXX/XXXX of the European Parliament and of the Council[29] [Resilience of Critical Entities Directive], or as an entity equivalent to a critical entity pursuant to Article 7 of that Directive.

   Member States shall establish a list of entities identified pursuant to points (b) to (f) and submit it to the Commission by [6 months after the transposition deadline]. Member States shall review the list, on a regular basis, and at least every two years thereafter and, where appropriate, update it.

3. This Directive is without prejudice to the competences of Member States concerning the maintenance of public security, defence and national security in compliance with Union law.

---

28 Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).

29 *[insert the full title and OJ publication reference when known]*

4. This Directive applies without prejudice to Council Directive 2008/114/EC[30] and Directives 2011/93/EU[31] and 2013/40/EU[32] of the European Parliament and of the Council.

5. Without prejudice to Article 346 TFEU, information that is confidential pursuant to Union and national rules, such as rules on business confidentiality, shall be exchanged with the Commission and other relevant authorities only where that exchange is necessary for the application of this Directive. The information exchanged shall be limited to that which is relevant and proportionate to the purpose of that exchange. The exchange of information shall preserve the confidentiality of that information and protect the security and commercial interests of essential or important entities.

6. Where provisions of sector–specific acts of Union law require essential or important entities either to adopt cybersecurity risk management measures or to notify incidents or significant cyber threats, and where those requirements are at least equivalent in effect to the obligations laid down in this Directive, the relevant provisions of this Directive, including the provision on supervision and enforcement laid down in Chapter VI, shall not apply.

Article 3

Minimum harmonisation

Without prejudice to their other obligations under Union law, Member States may, in accordance with this Directive, adopt or maintain provisions ensuring a higher level of cybersecurity.

Article 4

Definitions

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

(1) 'network and information system' means:

(a) an electronic communications network within the meaning of Article 2(1) of Directive (EU) 2018/1972;

(b) any device or group of inter–connected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data;

---

30 Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (OJ L 345, 23.12.2008, p. 75).

31 Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (OJ L 335, 17.12.2011, p. 1).

32 Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (OJ L 218, 14.8.2013, p. 8).

(c) digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance;

(2) 'security of network and information systems' means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems;

(3) 'cybersecurity' means cybersecurity within the meaning of Article 2(1) of Regulation (EU) 2019/881 of the European Parliament and of the Council[33];

(4) 'national strategy on cybersecurity' means a coherent framework of a Member State providing strategic objectives and priorities on the security of network and information systems in that Member State;

(5) 'incident' means any event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the related services offered by, or accessible via, network and information systems;

(6) 'incident handling' means all actions and procedures aiming at detection, analysis and containment of and a response to an incident;

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

(8) 'vulnerability' means a weakness, susceptibility or flaw of an asset, system, process or control that can be exploited by a cyber threat;

(9) 'representative' means any natural or legal person established in the Union explicitly designated to act on behalf of i) a DNS service provider, a top-level domain (TLD) name registry, a cloud computing service provider, a data centre service provider, a content delivery network provider as referred to in point 8 of Annex I or ii) entities referred to in point 6 of Annex II that are not established in the Union, which may be addressed by a national competent authority or a CSIRT instead of the entity with regard to the obligations of that entity under this Directive;

(10) 'standard' means a standard within the meaning of Article 2(1) of Regulation (EU) No 1025/2012 of the European Parliament and of the Council[34];

(11) 'technical specification' means a technical specification within the meaning of Article 2(4) of Regulation (EU) No 1025/2012;

(12) 'internet exchange point (IXP)' means a network facility which enables the interconnection of more than two independent networks (autonomous systems), primarily for the purpose of facilitating the exchange of internet traffic; an IXP

---

33 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).

34 Regulation (EU) No 1025/2012 of the European Parliament and of the Council 25 October 2012 on European standardization, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council (OJ L 316,14.11.2012,p.12).

provides interconnection only for autonomous systems; an IXP does not require the internet traffic passing between any pair of participating autonomous systems to pass through any third autonomous system, nor does it alter or otherwise interfere with such traffic;

(13) 'domain name system (DNS)' means a hierarchical distributed naming system which allows end-users to reach services and resources on the internet;

(14) 'DNS service provider' means an entity that provides recursive or authoritative domain name resolution services to internet end-users and other DNS service providers;

(15) 'top–level domain name registry' means an entity which has been delegated a specific TLD and is responsible for administering the TLD including the registration of domain names under the TLD and the technical operation of the TLD, including the operation of its name servers, the maintenance of its databases and the distribution of TLD zone files across name servers;

(16) 'digital service' means a service within the meaning of Article 1(1)(b) of Directive (EU) 2015/1535 of the European Parliament and of the Council [35];

(17) 'online marketplace' means a digital service within the meaning of Article 2 point (n) of Directive 2005/29/EC of the European Parliament and of the Council[36];

(18) 'online search engine' means a digital service within the meaning of Article 2(5) of Regulation (EU) 2019/1150 of the European Parliament and of the Council[37];

(19) 'cloud computing service' means a digital service that enables on-demand administration and broad remote access to a scalable and elastic pool of shareable and distributed computing resources;

(20) 'data centre service' means a service that encompasses structures, or groups of structures, dedicated to the centralised accommodation, interconnection and operation of information technology and network equipment providing data storage, processing and transport services together with all the facilities and infrastructures for power distribution and environmental control;

(21) 'content delivery network' means a network of geographically distributed servers for the purpose of ensuring high availability, accessibility or fast delivery of digital content and services to internet users on behalf of content and service providers;

(22) 'social networking services platform' means a platform that enables end-users to connect, share, discover and communicate with each other across multiple devices, and in particular, via chats, posts, videos and recommendations);

---

35 Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L. 241, 17.9.2015, p.1).

36 Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') (OJ L 149, 11.6.2005, p. 22).

37 Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services (OJ L 186, 11.7.2019, p. 57).

(23) ‘public administration entity’ means an entity in a Member State that complies with the following criteria:

(a) it is established for the purpose of meeting needs in the general interest and does not have an industrial or commercial character;

(b) it has legal personality;

(c) it is financed, for the most part, by the State, regional authority, or by other bodies governed by public law; or it is subject to management supervision by those authorities or bodies; or it has an administrative, managerial or supervisory board, more than half of whose members are appointed by the State, regional authorities, or by other bodies governed by public law;

(d) it has the power to address to natural or legal persons administrative or regulatory decisions affecting their rights in the cross-border movement of persons, goods, services or capital.

Public administration entities that carry out activities in the areas of public security, law enforcement, defence or national security are excluded.

(24) ‘entity’ means any natural or legal person created and recognised as such under the national law of its place of establishment, which may, acting under its own name, exercise rights and be subject to obligations;

(25) ‘essential entity’ means any entity of a type referred to as an essential entity in Annex I;

(26) ‘important entity’ means any entity of a type referred to as an important entity in Annex II.

CHAPTER II

Coordinated cybersecurity regulatory frameworks

Article 5
National cybersecurity strategy

1. Each Member State shall adopt a national cybersecurity strategy defining the strategic objectives and appropriate policy and regulatory measures, with a view to achieving and maintaining a high level of cybersecurity. The national cybersecurity strategy shall include, in particular, the following:

(a) a definition of objectives and priorities of the Member States’ strategy on cybersecurity;

(b) a governance framework to achieve those objectives and priorities, including the policies referred to in paragraph 2 and the roles and responsibilities of public bodies and entities as well as other relevant actors;

(c) an assessment to identify relevant assets and cybersecurity risks in that Member State;

(d) an identification of the measures ensuring preparedness, response and recovery to incidents, including cooperation between the public and private sectors;

(e) a list of the various authorities and actors involved in the implementation of the national cybersecurity strategy;

(f) a policy framework for enhanced coordination between the competent authorities under this Directive and Directive (EU) XXXX/XXXX of the European Parliament and of the Council[38] [Resilience of Critical Entities Directive] for the purposes of information sharing on incidents and cyber threats and the exercise of supervisory tasks.

2. As part of the national cybersecurity strategy, Member States shall in particular adopt the following policies:

(a) a policy addressing cybersecurity in the supply chain for ICT products and services used by essential and important entities for the provision of their services;

(b) guidelines regarding the inclusion and specification of cybersecurity-related requirements for ICT products and service in public procurement;

(c) a policy to promote and facilitate coordinated vulnerability disclosure within the meaning of Article 6;

(d) a policy related to sustaining the general availability and integrity of the public core of the open internet;

(e) a policy on promoting and developing cybersecurity skills, awareness raising and research and development initiatives;

(f) a policy on supporting academic and research institutions to develop cybersecurity tools and secure network infrastructure;

(g) a policy, relevant procedures and appropriate information-sharing tools to support voluntary cybersecurity information sharing between companies in compliance with Union law;

(h) a policy addressing specific needs of SMEs, in particular those excluded from the scope of this Directive, in relation to guidance and support in improving their resilience to cybersecurity threats.

3. Member States shall notify their national cybersecurity strategies to the Commission within three months from their adoption. Member States may exclude specific information from the notification where and to the extent that it is strictly necessary to preserve national security.

4. Member States shall assess their national cybersecurity strategies at least every four years on the basis of key performance indicators and, where necessary, amend them. The European Union Agency for Cybersecurity (ENISA) shall assist Member States, upon request, in the development of a national strategy and of key performance indicators for the assessment of the strategy.

Article 6

Coordinated vulnerability disclosure and a European vulnerability registry

[38] *[insert the full title and OJ publication reference when known]*

1. Each Member State shall designate one of its CSIRTs as referred to in Article 9 as a coordinator for the purpose of coordinated vulnerability disclosure. The designated CSIRT shall act as a trusted intermediary, facilitating, where necessary, the interaction between the reporting entity and the manufacturer or provider of ICT products or ICT services. Where the reported vulnerability concerns multiple manufacturers or providers of ICT products or ICT services across the Union, the designated CSIRT of each Member State concerned shall cooperate with the CSIRT network.

2. ENISA shall develop and maintain a European vulnerability registry. To that end, ENISA shall establish and maintain the appropriate information systems, policies and procedures with a view in particular to enabling important and essential entities and their suppliers of network and information systems to disclose and register vulnerabilities present in ICT products or ICT services, as well as to provide access to the information on vulnerabilities contained in the registry to all interested parties. The registry shall, in particular, include information describing the vulnerability, the affected ICT product or ICT services and the severity of the vulnerability in terms of the circumstances under which it may be exploited, the availability of related patches and, in the absence of available patches, guidance addressed to users of vulnerable products and services as to how the risks resulting from disclosed vulnerabilities may be mitigated.

Article 7

National cybersecurity crisis management frameworks

1. Each Member State shall designate one or more competent authorities responsible for the management of large-scale incidents and crises. Member States shall ensure that competent authorities have adequate resources to perform, in an effective and efficient manner, the tasks assigned to them.

2. Each Member State shall identify capabilities, assets and procedures that can be deployed in case of a crisis for the purposes of this Directive.

3. Each Member State shall adopt a national cybersecurity incident and crisis response plan where objectives and modalities in the management of large-scale cybersecurity incidents and crises are set out. The plan shall lay down, in particular, the following:

   (a) objectives of national preparedness measures and activities;

   (b) tasks and responsibilities of the national competent authorities;

   (c) crisis management procedures and information exchange channels;

   (d) preparedness measures, including exercises and training activities;

   (e) relevant public and private interested parties and infrastructure involved;

   (f) national procedures and arrangements between relevant national authorities and bodies to ensure the Member State's effective participation in and support of the coordinated management of large-scale cybersecurity incidents and crises at Union level.

4. Member States shall communicate to the Commission the designation of their competent authorities referred to in paragraph 1 and submit their national cybersecurity incident and crisis response plans as referred to in paragraph 3 within

three months from that designation and the adoption of those plans. Member States may exclude specific information from the plan where and to the extent that it is strictly necessary for their national security.

Article 8

National competent authorities and single points of contact

1. Each Member State shall designate one or more competent authorities responsible for cybersecurity and for the supervisory tasks referred to in Chapter VI of this Directive. Member States may designate to that effect an existing authority or existing authorities.
2. The competent authorities referred to paragraph 1 shall monitor the application of this Directive at national level.
3. Each Member State shall designate one national single point of contact on cybersecurity ('single point of contact'). Where a Member State designates only one competent authority, that competent authority shall also be the single point of contact for that Member State.
4. Each single point of contact shall exercise a liaison function to ensure cross–border cooperation of its Member State's authorities with the relevant authorities in other Member States, as well as to ensure cross-sectorial cooperation with other national competent authorities within its Member State.
5. Member States shall ensure that the competent authorities referred to in paragraph 1 and the single points of contact have adequate resources to carry out, in an effective and efficient manner, the tasks assigned to them and thereby to fulfil the objectives of this Directive. Member States shall ensure effective, efficient and secure cooperation of the designated representatives in the Cooperation Group referred to in Article 12.
6. Each Member State shall notify to the Commission, without undue delay, the designation of the competent authority referred to in paragraph 1 and single point of contact referred to in paragraph 3, their tasks, and any subsequent change thereto. Each Member State shall make public their designation. The Commission shall publish the list of the designated single points of contacts.

Article 9

Computer security incident response teams (CSIRTs)

1. Each Member State shall designate one or more CSIRTs which shall comply with the requirements set out in Article 10(1), covering at least the sectors, subsectors or entities referred to in Annexes I and II, and be responsible for incident handling in accordance with a well–defined process. A CSIRT may be established within a competent authority referred to in Article 8.
2. Member States shall ensure that each CSIRT has adequate resources to carry out effectively their tasks as set out in Article 10(2).
3. Member States shall ensure that each CSIRT has at its disposal an appropriate, secure, and resilient communication and information infrastructure to exchange

information with essential and important entities and other relevant interested parties. To this end, Member States shall ensure that the CSIRTs contribute to the deployment of secure information sharing tools.

4. CSIRTs shall cooperate and, where appropriate, exchange relevant information in accordance with Article 26 with trusted sectorial or cross-sectorial communities of essential and important entities.

5. CSIRTs shall participate in peer reviews organised in accordance with Article 16.

6. Member States shall ensure the effective, efficient and secure cooperation of their CSIRTs in the CSIRTs network referred to in Article 13.

7. Member States shall communicate to the Commission without undue delay the CSIRTs designated in accordance with paragraph 1, the CSIRT coordinator designated in accordance with Article 6(1) and their respective tasks provided in relation to the entities referred to in Annexes I and II.

8. Member States may request the assistance of ENISA in developing national CSIRTs.

Article 10

Requirements and tasks of CSIRTs

1. CSIRTs shall comply with the following requirements:

   (a) CSIRTs shall ensure a high level of availability of their communications services by avoiding single points of failure, and shall have several means for being contacted and for contacting others at all times. CSIRTs shall clearly specify the communication channels and make them known to constituency and cooperative partners;

   (b) CSIRTs' premises and the supporting information systems shall be located in secure sites;

   (c) CSIRTs shall be equipped with an appropriate system for managing and routing requests, in particular, to facilitate effective and efficient handovers;

   (d) CSIRTs shall be adequately staffed to ensure availability at all times;

   (e) CSIRTs shall be equipped with redundant systems and backup working space to ensure continuity of its services;

   (f) CSIRTs shall have the possibility to participate in international cooperation networks.

2. CSIRTs shall have the following tasks:

   (a) monitoring cyber threats, vulnerabilities and incidents at national level;

   (b) providing early warning, alerts, announcements and dissemination of information to essential and important entities as well as to other relevant interested parties on cyber threats, vulnerabilities and incidents;

   (c) responding to incidents;

   (d) providing dynamic risk and incident analysis and situational awareness regarding cybersecurity;

(e) providing, upon request of an entity, a proactive scanning of the network and information systems used for the provision of their services;

(f) participating in the CSIRTs network and providing mutual assistance to other members of the network upon their request.

3. CSIRTs shall establish cooperation relationships with relevant actors in the private sector, with a view to better achieving the objectives of the Directive.

4. In order to facilitate cooperation, CSIRTs shall promote the adoption and use of common or standardised practices, classification schemes and taxonomies in relation to the following:

(a) incident handling procedures;

(b) cybersecurity crisis management;

(c) coordinated vulnerability disclosure.

Article 11

Cooperation at national level

1. Where they are separate, the competent authorities referred to in Article 8, the single point of contact and the CSIRT(s) of the same Member State shall cooperate with each other with regard to the fulfilment of the obligations laid down in this Directive.

2. Member States shall ensure that either their competent authorities or their CSIRTs receive notifications on incidents, and significant cyber threats and near misses submitted pursuant to this Directive. Where a Member State decides that its CSIRTs shall not receive those notifications, the CSIRTs shall, to the extent necessary to carry out their tasks, be granted access to data on incidents notified by the essential or important entities, pursuant to Article 20.

3. Each Member State shall ensure that its competent authorities or CSIRTs inform its single point of contact of notifications on incidents, significant cyber threats and near misses submitted pursuant to this Directive.

4. To the extent necessary to effectively carry out the tasks and obligations laid down in this Directive, Member States shall ensure appropriate cooperation between the competent authorities and single points of contact and law enforcement authorities, data protection authorities, and the authorities responsible for critical infrastructure pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] and the national financial authorities designated in accordance with Regulation (EU) XXXX/XXXX of the European Parliament and of the Council[39] [the DORA Regulation] within that Member State.

5. Member States shall ensure that their competent authorities regularly provide information to competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] on cybersecurity risks, cyber threats and incidents affecting essential entities identified as critical, or as entities equivalent to critical entities, pursuant to Directive (EU) XXXX/XXXX

[39] *[insert the full title and OJ publication reference when known]*

[Resilience of Critical Entities Directive], as well as the measures taken by competent authorities in response to those risks and incidents.

CHAPTER III

Cooperation

Article 12
Cooperation Group

1. In order to support and to facilitate strategic cooperation and the exchange of information among Member States in the field of application of the Directive, a Cooperation Group is established.

2. The Cooperation Group shall carry out its tasks on the basis of biennial work programmes referred to in paragraph 6.

3. The Cooperation Group shall be composed of representatives of Member States, the Commission and ENISA. The European External Action Service shall participate in the activities of the Cooperation Group as an observer. The European Supervisory Authorities (ESAs) in accordance with Article 17(5)(c) of Regulation (EU) XXXX/XXXX [the DORA Regulation] may participate in the activities of the Cooperation Group.

   Where appropriate, the Cooperation Group may invite representatives of relevant stakeholders to participate in its work.

   The Commission shall provide the secretariat.

4. The Cooperation Group shall have the following tasks:

   (a) providing guidance to competent authorities in relation to the transposition and implementation of this Directive;

   (b) exchanging best practices and information in relation to the implementation of this Directive, including in relation to cyber threats, incidents, vulnerabilities, near misses, awareness-raising initiatives, trainings, exercises and skills, building capacity as well as standards and technical specifications;

   (c) exchanging advice and cooperating with the Commission on emerging cybersecurity policy initiatives;

   (d) exchanging advice and cooperating with the Commission on draft Commission implementing or delegated acts adopted pursuant to this Directive;

   (e) exchanging best practices and information with relevant Union institutions, bodies, offices and agencies;

   (f) discussing reports on the peer review referred to in Article 16(7);

   (g) discussing results from joint-supervisory activities in cross-border cases as referred to in Article 34;

(h) providing strategic guidance to the CSIRTs network on specific emerging issues;

(i) contributing to cybersecurity capabilities across the Union by facilitating the exchange of national officials through a capacity building programme involving staff from the Member States' competent authorities or CSIRTs;

(j) organising regular joint meetings with relevant private interested parties from across the Union to discuss activities carried out by the Group and gather input on emerging policy challenges;

(k) discussing the work undertaken in relation to cybersecurity exercises, including the work done by ENISA.

5. The Cooperation Group may request from the CSIRT network a technical report on selected topics.

6. By … [24 months after the date of entry into force of this Directive] and every two years thereafter, the Cooperation Group shall establish a work programme in respect of actions to be undertaken to implement its objectives and tasks. The timeframe of the first programme adopted under this Directive shall be aligned with the timeframe of the last programme adopted under Directive (EU) 2016/1148.

7. The Commission may adopt implementing acts laying down procedural arrangements necessary for the functioning of the Cooperation Group. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 37(2).

8. The Cooperation Group shall meet regularly and at least once a year with the Critical Entities Resilience Group established under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] to promote strategic cooperation and exchange of information.

Article 13
CSIRTs network

1. In order to contribute to the development of confidence and trust and to promote swift and effective operational cooperation among Member States, a network of the national CSIRTs is established.

2. The CSIRTs network shall be composed of representatives of the Member States' CSIRTs and CERT–EU. The Commission shall participate in the CSIRTs network as an observer. ENISA shall provide the secretariat and shall actively support cooperation among the CSIRTs.

3. The CSIRTs network shall have the following tasks:

(a) exchanging information on CSIRTs' capabilities;

(b) exchanging relevant information on incidents, near misses, cyber threats, risks and vulnerabilities;

(c) at the request of a representative of the CSIRT network potentially affected by an incident, exchanging and discussing information in relation to that incident and associated cyber threats, risks and vulnerabilities;

(d) at the request of a representative of the CSIRT network, discussing and, where possible, implementing a coordinated response to an incident that has been identified within the jurisdiction of that Member State;

(e) providing Member States with support in addressing cross–border incidents pursuant to this Directive;

(f) cooperating and providing assistance to designated CSIRTs referred to in Article 6 with regard to the management of multiparty coordinated disclosure of vulnerabilities affecting multiple manufacturers or providers of ICT products, ICT services and ICT processes established in different Member States;

(g) discussing and identifying further forms of operational cooperation, including in relation to:

(i) categories of cyber threats and incidents;

(ii) early warnings;

(iii) mutual assistance;

(iv) principles and modalities for coordination in response to cross–border risks and incidents;

(v) contribution to the national cybersecurity incident and crisis response plan referred to in Article 7 (3);

(h) informing the Cooperation Group of its activities and of the further forms of operational cooperation discussed pursuant to point (g), where necessary, requesting guidance in that regard;

(i) taking stock from cybersecurity exercises, including from those organised by ENISA;

(j) at the request of an individual CSIRT, discussing the capabilities and preparedness of that CSIRT;

(k) cooperating and exchanging information with regional and Union-level Security Operations Centres (SOCs) in order to improve common situational awareness on incidents and threats across the Union;

(l) discussing the peer-review reports referred to in Article 16(7);

(m) issuing guidelines in order to facilitate the convergence of operational practices with regard to the application of the provisions of this Article concerning operational cooperation.

4. For the purpose of the review referred to in Article 35 and by [24 months after the date of entry into force of this Directive], and every two years thereafter, the CSIRTs network shall assess the progress made with the operational cooperation and produce a report. The report shall, in particular, draw conclusions on the outcomes of the peer reviews referred to in Article 16 carried out in relation to national CSIRTs, including conclusions and recommendations, pursued under this Article. That report shall also be submitted to the Cooperation Group.

5. The CSIRTs network shall adopt its own rules of procedure.

Article 14

The European cyber crises liaison organisation network (EU - CyCLONe)

1. In order to support the coordinated management of large-scale cybersecurity incidents and crises at operational level and to ensure the regular exchange of information among Member States and Union institutions, bodies and agencies, the European Cyber Crises Liaison Organisation Network (EU - CyCLONe) is hereby established.
2. EU-CyCLONe shall be composed of the representatives of Member States' crisis management authorities designated in accordance with Article 7, the Commission and ENISA. ENISA shall provide the secretariat of the network and support the secure exchange of information.
3. EU-CyCLONe shall have the following tasks:
   (a) increasing the level of preparedness of the management of large scale incidents and crises;
   (b) developing a shared situational awareness of relevant cybersecurity events;
   (c) coordinating large scale incidents and crisis management and supporting decision-making at political level in relation to such incidents and crisis;
   (d) discussing national cybersecurity incident and response plans referred to in Article 7(2).
4. EU-CyCLONe shall adopt its rules of procedure.
5. EU-CyCLONe shall regularly report to the Cooperation Group on cyber threats, incidents and trends, focusing in particular on their impact on essential and important entities.
6. EU-CyCLONe shall cooperate with the CSIRTs network on the basis of agreed procedural arrangements.

Article 15

Report on the state of cybersecurity in the Union

1. ENISA shall issue, in cooperation with the Commission, a biennial report on the state of cybersecurity in the Union. The report shall in particular include an assessment of the following:
   (a) the development of cybersecurity capabilities across the Union;
   (b) the technical, financial and human resources available to competent authorities and cybersecurity policies, and the implementation of supervisory measures and enforcement actions in light of the outcomes of peer reviews referred to in Article 16;
   (c) a cybersecurity index providing for an aggregated assessment of the maturity level of cybersecurity capabilities.
2. The report shall include particular policy recommendations for increasing the level of cybersecurity across the Union and a summary of the findings for the particular

period from the Agency's EU Cybersecurity Technical Situation Reports issued by ENISA in accordance with Article 7(6) of Regulation (EU) 2019/881.

Article 16

Peer-reviews

1. The Commission shall establish, after consulting the Cooperation Group and ENISA, and at the latest by 18 months following the entry into force of this Directive, the methodology and content of a peer-review system for assessing the effectiveness of the Member States' cybersecurity policies. The reviews shall be conducted by cybersecurity technical experts drawn from Member States different than the one reviewed and shall cover at least the following:

   (i) the effectiveness of the implementation of the cybersecurity risk management requirements and reporting obligations referred to in Articles 18 and 20;

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

   (iii) the operational capabilities and effectiveness of CSIRTs;

   (iv) the effectiveness of mutual assistance referred to in Article 34;

   (v) the effectiveness of the information-sharing framework, referred to in Article 26 of this Directive.

2. The methodology shall include objective, non-discriminatory, fair and transparent criteria on the basis of which the Member States shall designate experts eligible to carry out the peer reviews. ENISA and the Commission shall designate experts to participate as observers in the peer-reviews. The Commission, supported by ENISA, shall establish within the methodology as referred to in paragraph 1 an objective, non-discriminatory, fair and transparent system for the selection and the random allocation of experts for each peer review.

3. The organisational aspects of the peer reviews shall be decided by the Commission, supported by ENISA, and, following consultation of the Cooperation Group, be based on criteria defined in the methodology referred to in paragraph 1. Peer reviews shall assess the aspects referred to in paragraph 1 for all Member States and sectors, including targeted issues specific to one or several Member States or one or several sectors.

4. Peer reviews shall entail actual or virtual on-site visits and off-site exchanges. In view of the principle of good cooperation, the Member States being reviewed shall provide the designated experts with the requested information necessary for the assessment of the reviewed aspects. Any information obtained through the peer review process shall be used solely for that purpose. The experts participating in the peer review shall not disclose any sensitive or confidential information obtained in the course of that review to any third parties.

5. Once reviewed in a Member State, the same aspects shall not be subject to further peer review within that Member State during the two years following the conclusion of a peer review, unless otherwise decided by the Commission, upon consultation with ENISA and the Cooperation Group.

6. Member State shall ensure that any risk of conflict of interests concerning the designated experts are revealed to the other Member States, the Commission and ENISA without undue delay.

7. Experts participating in peer reviews shall draft reports on the findings and conclusions of the reviews. The reports shall be submitted to the Commission, the Cooperation Group, the CSIRTs network and ENISA. The reports shall be discussed in the Cooperation Group and the CSIRTs network. The reports may be published on the dedicated website of the Cooperation Group.

CHAPTER IV

Cybersecurity risk management and reporting obligations

SECTION I

Cybersecurity risk management and reporting

Article 17

Governance

1. Member States shall ensure that the management bodies of essential and important entities approve the cybersecurity risk management measures taken by those entities in order to comply with Article 18, supervise its implementation and be accountable for the non-compliance by the entities with the obligations under this Article.

2. Member States shall ensure that members of the management body follow specific trainings, on a regular basis, to gain sufficient knowledge and skills in order to apprehend and assess cybersecurity risks and management practices and their impact on the operations of the entity.

Article 18

Cybersecurity risk management measures

1. Member States shall ensure that essential and important entities shall take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which those entities use in the provision of their services. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk presented.

2. The measures referred to in paragraph 1 shall include at least the following:

   (a) risk analysis and information system security policies;

   (b) incident handling (prevention, detection, and response to incidents);

   (c) business continuity and crisis management;

(d) supply chain security including security-related aspects concerning the relationships between each entity and its suppliers or service providers such as providers of data storage and processing services or managed security services;

(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

(f) policies and procedures (testing and auditing) to assess the effectiveness of cybersecurity risk management measures;

(g) the use of cryptography and encryption.

3. Member States shall ensure that, where considering appropriate measures referred to in point (d) of paragraph 2, entities shall take into account the vulnerabilities specific to each supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures.

4. Member States shall ensure that where an entity finds that respectively its services or tasks are not in compliance with the requirements laid down in paragraph 2, it shall, without undue delay, take all necessary corrective measures to bring the service concerned into compliance.

5. The Commission may adopt implementing acts in order to lay down the technical and the methodological specifications of the elements referred to in paragraph 2. Where preparing those acts, the Commission shall proceed in accordance with the examination procedure referred to in Article 37(2) and follow, to the greatest extent possible, international and European standards, as well as relevant technical specifications.

6. The Commission is empowered to adopt delegated acts in accordance with Article 36 to supplement the elements laid down in paragraph 2 to take account of new cyber threats, technological developments or sectorial specificities.

Article 19

EU coordinated risk assessments of critical supply chains

1. The Cooperation Group, in cooperation with the Commission and ENISA, may carry out coordinated security risk assessments of specific critical ICT services, systems or products supply chains, taking into account technical and, where relevant, non-technical risk factors.

2. The Commission, after consulting with the Cooperation Group and ENISA, shall identify the specific critical ICT services, systems or products that may be subject to the coordinated risk assessment referred to in paragraph 1.

Article 20

Reporting obligations

1. Member States shall ensure that essential and important entities notify, without undue delay, the competent authorities or the CSIRT in accordance with paragraphs

3 and 4 of any incident having a significant impact on the provision of their services. Where appropriate, those entities shall notify, without undue delay, the recipients of their services of incidents that are likely to adversely affect the provision of that service. Member States shall ensure that those entities report, among others, any information enabling the competent authorities or the CSIRT to determine any cross-border impact of the incident.

2. Member States shall ensure that essential and important entities notify, without undue delay, the competent authorities or the CSIRT of any significant cyber threat that those entities identify that could have potentially resulted in a significant incident.

Where applicable, those entities shall notify, without undue delay, the recipients of their services that are potentially affected by a significant cyber threat of any measures or remedies that those recipients can take in response to that threat. Where appropriate, the entities shall also notify those recipients of the threat itself. The notification shall not make the notifying entity subject to increased liability.

3. An incident shall be considered significant if:

(a) the incident has caused or has the potential to cause substantial operational disruption or financial losses for the entity concerned;

(b) the incident has affected or has the potential to affect other natural or legal persons by causing considerable material or non-material losses.

4. Member States shall ensure that, for the purpose of the notification under paragraph 1, the entities concerned shall submit to the competent authorities or the CSIRT:

(a) without undue delay and in any event within 24 hours after having become aware of the incident, an initial notification, which, where applicable, shall indicate whether the incident is presumably caused by unlawful or malicious action;

(b) upon the request of a competent authority or a CSIRT, an intermediate report on relevant status updates;

(c) a final report not later than one month after the submission of the report under point (a), including at least the following:

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

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

(iii) applied and ongoing mitigation measures.

Member States shall provide that in duly justified cases and in agreement with the competent authorities or the CSIRT, the entity concerned can deviate from the deadlines laid down in points (a) and (c).

5. The competent national authorities or the CSIRT shall provide, within 24 hours after receiving the initial notification referred to in point (a) of paragraph 4, a response to the notifying entity, including initial feedback on the incident and, upon request of the entity, guidance on the implementation of possible mitigation measures. Where the CSIRT did not receive the notification referred to in paragraph 1 , the guidance shall be provided by the competent authority in collaboration with the CSIRT. The CSIRT shall provide additional technical support if the concerned entity so requests. Where the incident is suspected to be of criminal nature, the competent national

authorities or the CSIRT shall also provide guidance on reporting the incident to law enforcement authorities.

6. Where appropriate, and in particular where the incident referred to in paragraph 1 concerns two or more Member States, the competent authority or the CSIRT shall inform the other affected Member States and ENISA of the incident. In so doing, the competent authorities, CSIRTs and single points of contact shall, in accordance with Union law or national legislation that complies with Union law, preserve the entity's security and commercial interests as well as the confidentiality of the information provided.

7. Where public awareness is necessary to prevent an incident or to deal with an ongoing incident, or where disclosure of the incident is otherwise in the public interest, the competent authority or the CSIRT, and where appropriate the authorities or the CSIRTs of other Member States concerned may, after consulting the entity concerned, inform the public about the incident or require the entity to do so.

8. At the request of the competent authority or the CSIRT, the single point of contact shall forward notifications received pursuant to paragraphs 1 and 2 to the single points of contact of other affected Member States.

9. The single point of contact shall submit to ENISA on a monthly basis a summary report including anonymised and aggregated data on incidents, significant cyber threats and near misses notified in accordance with paragraphs 1 and 2 and in accordance with Article 27. In order to contribute to the provision of comparable information, ENISA may issue technical guidance on the parameters of the information included in the summary report.

10. Competent authorities shall provide to the competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] information on incidents and cyber threats notified in accordance with paragraphs 1 and 2 by essential entities identified as critical entities, or as entities equivalent to critical entities, pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive].

11. The Commission, may adopt implementing acts further specifying the type of information, the format and the procedure of a notification submitted pursuant to paragraphs 1 and 2. The Commission may also adopt implementing acts to further specify the cases in which an incident shall be considered significant as referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 37(2).

Article 21

Use of European cybersecurity certification schemes

1. In order to demonstrate compliance with certain requirements of Article 18, Member States may require essential and important entities to certify certain ICT products, ICT services and ICT processes under specific European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881. The products, services and processes subject to certification may be developed by an essential or important entity or procured from third parties.

2. The Commission shall be empowered to adopt delegated acts specifying which categories of essential entities shall be required to obtain a certificate and under which specific European cybersecurity certification schemes pursuant to paragraph 1. The delegated acts shall be adopted in accordance with Article 36.

3. The Commission may request ENISA to prepare a candidate scheme pursuant to Article 48(2) of Regulation (EU) 2019/881 in cases where no appropriate European cybersecurity certification scheme for the purposes of paragraph 2 is available.

Article 22

Standardisation

1. In order to promote the convergent implementation of Article 18(1) and (2), Member States shall, without imposing or discriminating in favour of the use of a particular type of technology, encourage the use of European or internationally accepted standards and specifications relevant to the security of network and information systems.

2. ENISA, in collaboration with Member States, shall draw up advice and guidelines regarding the technical areas to be considered in relation to paragraph 1 as well as regarding already existing standards, including Member States' national standards, which would allow for those areas to be covered.

Article 23

Databases of domain names and registration data

1. For the purpose of contributing to the security, stability and resilience of the DNS, Member States shall ensure that TLD registries and the entities providing domain name registration services for the TLD shall collect and maintain accurate and complete domain name registration data in a dedicated database facility with due diligence subject to Union data protection law as regards data which are personal data.

2. Member States shall ensure that the databases of domain name registration data referred to in paragraph 1 contain relevant information to identify and contact the holders of the domain names and the points of contact administering the domain names under the TLDs.

3. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD have policies and procedures in place to ensure that the databases include accurate and complete information. Member States shall ensure that such policies and procedures are made publicly available.

4. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD publish, without undue delay after the registration of a domain name, domain registration data which are not personal data.

5. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD provide access to specific domain name registration data upon lawful and duly justified requests of legitimate access seekers, in compliance with Union data protection law. Member States shall ensure that the

TLD registries and the entities providing domain name registration services for the TLD reply without undue delay to all requests for access. Member States shall ensure that policies and procedures to disclose such data are made publicly available.

Section II

Jurisdiction and Registration

Article 24

Jurisdiction and territoriality

1. DNS service providers, TLD name registries, cloud computing service providers, data centre service providers and content delivery network providers referred to in point 8 of Annex I, as well as digital providers referred to in point 6 of Annex II shall be deemed to be under the jurisdiction of the Member State in which they have their main establishment in the Union.

2. For the purposes of this Directive, entities referred to in paragraph 1 shall be deemed to have their main establishment in the Union in the Member State where the decisions related to the cybersecurity risk management measures are taken. If such decisions are not taken in any establishment in the Union, the main establishment shall be deemed to be in the Member State where the entities have the establishment with the highest number of employees in the Union.

3. If an entity referred to in paragraph 1 is not established in the Union, but offers services within the Union, it shall designate a representative in the Union. The representative shall be established in one of those Member States where the services are offered. Such entity shall be deemed to be under the jurisdiction of the Member State where the representative is established. In the absence of a designated representative within the Union under this Article, any Member State in which the entity provides services may take legal actions against the entity for non-compliance with the obligations under this Directive.

4. The designation of a representative by an entity referred to in paragraph 1 shall be without prejudice to legal actions, which could be initiated against the entity itself.

Article 25

Registry for essential and important entities

1. ENISA shall create and maintain a registry for essential and important entities referred to in Article 24(1). The entities shall submit the following information to ENISA by [12 months after entering into force of the Directive at the latest]:

   (a) the name of the entity;

   (b) the address of its main establishment and its other legal establishments in the Union or, if not established in the Union, of its representative designated pursuant to Article 24(3);

   (c) up-to-date contact details, including email addresses and telephone numbers of the entities.

2. The entities referred to in paragraph 1 shall notify ENISA about any changes to the details they submitted under paragraph 1 without delay, and in any event, within three months from the date on which the change took effect.

3. Upon receipt of the information under paragraph 1, ENISA shall forward it to the single points of contact depending on the indicated location of each entity's main establishment or, if it is not established in the Union, of its designated representative. Where an entity referred to in paragraph 1 has besides its main establishment in the Union further establishments in other Member States, ENISA shall also inform the single points of contact of those Member States.

4. Where an entity fails to register its activity or to provide the relevant information within the deadline set out in paragraph 1, any Member State where the entity provides services shall be competent to ensure that entity's compliance with the obligations laid down in this Directive.

CHAPTER V

Information sharing

Article 26

Cybersecurity information-sharing arrangements

1. Without prejudice to Regulation (EU) 2016/679, Member States shall ensure that essential and important entities may exchange relevant cybersecurity information among themselves including information relating to cyber threats, vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools, where such information sharing:

   (a) aims at preventing, detecting, responding to or mitigating incidents;

   (b) enhances the level of cybersecurity, in particular through raising awareness in relation to cyber threats, limiting or impeding such threats 'ability to spread, supporting a range of defensive capabilities, vulnerability remediation and disclosure, threat detection techniques, mitigation strategies, or response and recovery stages.

2. Member States shall ensure that the exchange of information takes place within trusted communities of essential and important entities. Such exchange shall be implemented through information sharing arrangements in respect of the potentially sensitive nature of the information shared and in compliance with the rules of Union law referred to in paragraph 1.

3. Member States shall set out rules specifying the procedure, operational elements (including the use of dedicated ICT platforms), content and conditions of the information sharing arrangements referred to in paragraph 2. Such rules shall also lay down the details of the involvement of public authorities in such arrangements, as well as operational elements, including the use of dedicated IT platforms. Member States shall offer support to the application of such arrangements in accordance with their policies referred to in Article 5(2) (g).

4. Essential and important entities shall notify the competent authorities of their participation in the information-sharing arrangements referred to in paragraph 2, upon entering into such arrangements, or, as applicable, of their withdrawal from such arrangements, once the withdrawal takes effect.

5. In compliance with Union law, ENISA shall support the establishment of cybersecurity information-sharing arrangements referred to in paragraph 2 by providing best practices and guidance.

Article 27

Voluntary notification of relevant information

Member States shall ensure that, without prejudice to Article 3, entities falling outside the scope of this Directive may submit notifications, on a voluntary basis, of significant incidents, cyber threats or near misses. When processing notifications, Member States shall act in accordance with the procedure laid down in Article 20. Member States may prioritise the processing of mandatory notifications over voluntary notifications. Voluntary reporting shall not result in the imposition of any additional obligations upon the reporting entity to which it would not have been subject had it not submitted the notification.

CHAPTER VI

Supervision and enforcement

Article 28

General aspects concerning supervision and enforcement

1. Member States shall ensure that competent authorities effectively monitor and take the measures necessary to ensure compliance with this Directive, in particular the obligations laid down in Articles 18 and 20.

2. Competent authorities shall work in close cooperation with data protection authorities when addressing incidents resulting in personal data breaches.

Article 29

Supervision and enforcement for essential entities

1. Member States shall ensure that the measures of supervision or enforcement imposed on essential entities in respect of the obligations set out in this Directive are effective, proportionate and dissuasive, taking into account the circumstances of each individual case.

2. Member States shall ensure that competent authorities, where exercising their supervisory tasks in relation to essential entities, have the power to subject those entities to:

   (a) on-site inspections and off-site supervision, including random checks;

   (b) regular audits;

(c) targeted security audits based on risk assessments or risk-related available information;

(d) security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria;

(e) requests of information necessary to assess the cybersecurity measures adopted by the entity, including documented cybersecurity policies, as well as compliance with the obligation to notify the ENISA pursuant to Article 25 (1) and (2);

(f) requests to access data, documents or any information necessary for the performance of their supervisory tasks;

(g) requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence.

3. Where exercising their powers under points (e) to (g) of paragraph 2, the competent authorities shall state the purpose of the request and specify the information requested.

4. Member States shall ensure that competent authorities, where exercising their enforcement powers in relation to essential entities, have the power to:

(a) issue warnings on the entities' non-compliance with the obligations laid down in this Directive;

(b) issue binding instructions or an order requiring those entities to remedy the deficiencies identified or the infringements of the obligations laid down in this Directive;

(c) order those entities to cease conduct that is non-compliant with the obligations laid down in this Directive and desist from repeating that conduct;

(d) order those entities to bring their risk management measures and/or reporting obligations in compliance with the obligations laid down in Articles 18 and 20 in a specified manner and within a specified period;

(e) order those entities to inform the natural or legal person(s) to whom they provide services or activities which are potentially affected by a significant cyber threat of any possible protective or remedial measures which can be taken by those natural or legal person(s) in response to that threat;

(f) order those entities to implement the recommendations provided as a result of a security audit within a reasonable deadline;

(g) designate a monitoring officer with well-defined tasks over a determined period of time to oversee the compliance with their obligations provided for by Articles 18 and 20;

(h) order those entities to make public aspects of non-compliance with the obligations laid down in this Directive in a specified manner;

(i) make a public statement which identifies the legal and natural person(s) responsible for the infringement of an obligation laid down in this Directive and the nature of that infringement;

(j) impose or request the imposition by the relevant bodies or courts according to national laws of an administrative fine pursuant to Article 31 in addition to, or

instead of, the measures referred to in points (a) to (i) of this paragraph, depending on the circumstances of each individual case.

5. Where enforcement actions adopted pursuant to points (a) to (d) and (f) of paragraph (4) prove ineffective, Member States shall ensure that competent authorities have the power to establish a deadline within which the essential entity is requested to take the necessary action to remedy the deficiencies or comply with the requirements of those authorities. If the requested action is not taken within the deadline set, Member States shall ensure that the competent authorities have the power to:

   (a) suspend or request a certification or authorisation body to suspend a certification or authorisation concerning part or all the services or activities provided by an essential entity;

   (b) impose or request the imposition by the relevant bodies or courts according to national laws of a temporary ban against any person discharging managerial responsibilities at chief executive officer or legal representative level in that essential entity, and of any other natural person held responsible for the breach, from exercising managerial functions in that entity.

   These sanctions shall be applied only until the entity takes the necessary action to remedy the deficiencies or comply with the requirements of the competent authority for which such sanctions were applied.

6. Member States shall ensure that any natural person responsible for or acting as a representative of an essential entity on the basis of the power to represent it, the authority to take decisions on its behalf or the authority to exercise control of it has the powers to ensure its compliance with the obligations laid down in this Directive. Member States shall ensure that those natural persons may be held liable for breach of their duties to ensure compliance with the obligations laid down in this Directive.

7. Where taking any of the enforcement actions or applying any sanctions pursuant to paragraphs 4 and 5, the competent authorities shall comply with the rights of the defence and take account of the circumstances of each individual case and, as a minimum, take due account of:

   (a) the seriousness of the infringement and the importance of the provisions breached. Among the infringements that should be considered as serious: repeated violations, failure to notify or remedy incidents with a significant disruptive effect, failure to remedy deficiencies following binding instructions from competent authorities obstruction of audits or monitoring activities ordered by the competent authority following the finding of an infringement, providing false or grossly inaccurate information in relation to risk management requirements or reporting obligations set out in Articles 18 and 20.

   (b) the duration of the infringement, including the element of repeated infringements;

   (c) the actual damage caused or losses incurred or potential damage or losses that could have been triggered, insofar as they can be determined. Where evaluating this aspect, account shall be taken, amongst others, of actual or potential financial or economic losses, effects on other services, number of users affected or potentially affected;

   (d) the intentional or negligent character of the infringement;

(e) measures taken by the entity to prevent or mitigate the damage and/or losses;

(f) adherence to approved codes of conduct or approved certification mechanisms;

(g) the level of cooperation of the natural or legal person(s) held responsible with the competent authorities.

8. The competent authorities shall set out a detailed reasoning for their enforcement decisions. Before taking such decisions, the competent authorities shall notify the entities concerned of their preliminary findings and allow a reasonable time for those entities to submit observations.

9. Member States shall ensure that their competent authorities inform the relevant competent authorities of the Member State concerned designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] when exercising their supervisory and enforcement powers aimed at ensuring compliance of an essential entity identified as critical, or as an entity equivalent to a critical entity, under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] with the obligations pursuant to this Directive. Upon request of competent authorities under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive], competent authorities may exercise their supervisory and enforcement powers on an essential entity identified as critical or equivalent.

Article 30

Supervision and enforcement for important entities

1. When provided with evidence or indication that an important entity is not in compliance with the obligations laid down in this Directive, and in particular in Articles 18 and 20, Member States shall ensure that the competent authorities take action, where necessary, through *ex post* supervisory measures.

2. Member States shall ensure that the competent authorities, where exercising their supervisory tasks in relation to important entities, have the power to subject those entities to:

(a) on-site inspections and off-site *ex post* supervision;

(b) targeted security audits based on risk assessments or risk-related available information;

(c) security scans based on objective, fair and transparent risk assessment criteria;

(d) requests for any information necessary to assess ex-post the cybersecurity measures, including documented cybersecurity policies, as well as compliance with the obligation to notify ENISA pursuant to Article 25(1) and (2);

(e) requests to access data, documents and/or information necessary for the performance of the supervisory tasks.

3. Where exercising their powers pursuant to points (d) or (e) of paragraph 2, the competent authorities shall state the purpose of the request and specify the information requested.

4. Member States shall ensure that the competent authorities, where exercising their enforcement powers in relation to important entities, have the power to:

(a) issue warnings on the entities' non-compliance with the obligations laid down in this Directive;

(b) issue binding instructions or an order requiring those entities to remedy the deficiencies identified or the infringement of the obligations laid down in this Directive;

(c) order those entities to cease conduct that is in non-compliant with the obligations laid down in this Directive and desist from repeating that conduct;

(d) order those entities to bring their risk management measures or the reporting obligations in compliance with the obligations laid down in Articles 18 and 20 in a specified manner and within a specified period;

(e) order those entities to inform the natural or legal person(s) to whom they provide services or activities which are potentially affected by a significant cyber threat of any possible protective or remedial measures which can be taken by those natural or legal person(s) in response to that threat;

(f) order those entities to implement the recommendations provided as a result of a security audit within a reasonable deadline;

(g) order those entities to make public aspects of non-compliance with their obligations laid down in this Directive in a specified manner;

(h) make a public statement which identifies the legal and natural person(s) responsible for the infringement of an obligation laid down in this Directive and the nature of that infringement;

(i) impose or request the imposition by the relevant bodies or courts according to national laws of an administrative fine pursuant to Article 31 in addition to, or instead of, the measures referred to in points (a) to (h) of this paragraph, depending on the circumstances of each individual case.

5. Article 29 (6) to (8) shall also apply to the supervisory and enforcement measures provided for in this Article for the important entities listed in Annex II.

Article 31

General conditions for imposing administrative fines on essential and important entities

1. Member States shall ensure that the imposition of administrative fines on essential and important entities pursuant to this Article in respect of infringements of the obligations laid down in this Directive are, in each individual case, effective, proportionate and dissuasive.

2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (i) of Article 29(4), Article 29(5) and points (a) to (h) of Article 30(4).

3. Where deciding whether to impose an administrative fine and deciding on its amount in each individual case due regard shall be given, as a minimum, to the elements provided for in Article 29(7).

4. Member States shall ensure that infringements of the obligations laid down in Article 18 or Article 20 shall, in accordance with paragraphs 2 and 3 of this Article, be subject to administrative fines of a maximum of at least 10 000 000 EUR or up to 2%

of the total worldwide annual turnover of the undertaking to which the essential or important entity belongs in the preceding financial year, whichever is higher.

5. Member States may provide for the power to impose periodic penalty payments in order to compel an essential or important entity to cease an infringement in accordance with a prior decision of the competent authority.

6. Without prejudice to the powers of competent authorities pursuant to Articles 29 and 30, each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public administration entities referred to in Article 4(23) subject to the obligations provided for by this Directive.

Article 32

Infringements entailing a personal data breach

1. Where the competent authorities have indications that the infringement by an essential or important entity of the obligations laid down in Articles 18 and 20 entails a personal data breach, as defined by Article 4(12) of Regulation (EU) 2016/679 which shall be notified pursuant to Article 33 of that Regulation, they shall inform the supervisory authorities competent pursuant to Articles 55 and 56 of that Regulation within a reasonable period of time.

2. Where the supervisory authorities competent in accordance with Articles 55 and 56 of Regulation (EU) 2016/679 decide to exercise their powers pursuant to Article 58(i) of that Regulation and impose an administrative fine, the competent authorities shall not impose an administrative fine for the same infringement under Article 31 of this Directive. The competent authorities may, however, apply the enforcement actions or exercise the sanctioning powers provided for in points (a) to (i) of Article 29 (4), Article 29 (5), and points (a) to (h) of Article 30 (4) of this Directive.

3. Where the supervisory authority competent pursuant to Regulation (EU) 2016/679 is established in another Member State than the competent authority, the competent authority may inform the supervisory authority established in the same Member State.

Article 33

Penalties

1. Member States shall lay down rules on penalties applicable to the infringements of national provisions adopted pursuant to this Directive, and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive.

2. Member States shall, by [two] years following the entry into force of this Directive, notify the Commission of those rules and of those measures and shall notify it, without undue delay of any subsequent amendment affecting them.

Article 34

Mutual assistance

1. Where an essential or important entity is providing services in more than one Member State, or has its main establishment or a representative in a Member State, but its network and information systems are located in one or more other Member States, the competent authority of the Member State of the main establishment or other establishment or of the representative, and the competent authorities of those other Member States shall cooperate with and assist each other as necessary. That cooperation shall entail, at least, that:

   (a) the competent authorities applying supervisory or enforcement measures in a Member State shall, via the single point of contact, inform and consult the competent authorities in the other Member States concerned on the supervisory and enforcement measures taken and their follow-up, in accordance with Articles 29 and 30;

   (b) a competent authority may request another competent authority to take the supervisory or enforcement measures referred to in Articles 29 and 30;

   (c) a competent authority shall, upon receipt of a justified request from another competent authority, provide the other competent authority with assistance so that the supervision or enforcement actions referred to in Articles 29 and 30 can be implemented in an effective, efficient and consistent manner. Such mutual assistance may cover information requests and supervisory measures, including requests to carry out on-site inspections or off-site supervision or targeted security audits. A competent authority to which a request for assistance is addressed may not refuse that request unless, after an exchange with the other authorities concerned, ENISA and the Commission, it is established that either the authority is not competent to provide the requested assistance or the requested assistance is not proportionate to the supervisory tasks of the competent authority carried out in accordance with Article 29 or Article 30.

2. Where appropriate and with common agreement, competent authorities from different Member States may carry out the joint supervisory actions referred to in Articles 29 and 30.

CHAPTER VII

Transitional and final provisions

Article 35

Review

The Commission shall periodically review the functioning of this Directive, and report to the European Parliament and to the Council. The report shall in particular assess the relevance of sectors, subsectors, size and type of entities referred to in Annexes I and II for the functioning of the economy and society in relation to cybersecurity. For this purpose and with a view to further advancing the strategic and operational cooperation, the Commission shall take into account the reports of the Cooperation Group and the CSIRTs network on the experience

gained at a strategic and operational level. The first report shall be submitted by… [54 months after the date of entry into force of this Directive].

Article 36

Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.
2. The power to adopt delegated acts referred to in Articles 18(6) and 21(2) shall be conferred on the Commission for a period of five years from […]
3. The delegation of power referred to in Articles 18(6) and 21(2) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.
4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with principles laid down in the Inter-institutional Agreement of 13 April 2016 on Better Law-Making.
5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.
6. A delegated act adopted pursuant to Articles 18(6) and 21(2) shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of two months of notification of that act to the European Parliament and to the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

Article 37

Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.
2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.
3. Where the opinion of the committee is to be obtained by written procedure, that procedure shall be terminated without result when, within the time-limit for delivery of the opinion, the chair of the committee so decides or a committee member so requests.

Article 38

Transposition

1. Member States shall adopt and publish, by … [18 months after the date of entry into force of this Directive], the laws, regulations and administrative provisions necessary to comply with this Directive. They shall immediately inform the Commission thereof. They shall apply those measures from … [one day after the date referred to in the first subparagraph].
2. When Member States adopt those measures, they shall contain a reference to this Directive or shall be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.

Article 39

Amendment of Regulation (EU) No 910/2014

Article 19 of Regulation (EU) No 910/2014 is deleted.

Article 40

Amendment of Directive (EU) 2018/1972

Articles 40 and 41 of Directive (EU) 2018/1972 are deleted.

Article 41

Repeal

Directive (EU) 2016/1148 is repealed with effect from.. [date of transposition deadline of the Directive].

References to Directive (EU) 2016/1148 shall be construed as references to this Directive and read in accordance with the correlation table set out in Annex III.

Article 42

Entry into force

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

Article 43

Addressees

This Directive is addressed to the Member States.

Done at Brussels,

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

LEGISLATIVE FINANCIAL STATEMENT

Contents

1. FRAMEWORK OF THE PROPOSAL/INITIATIVE 2
1.1. Title of the proposal/initiative 2
1.2. Policy area(s) concerned *(Programme cluster)* 2
1.3. The proposal/initiative relates to: 2
1.4. Grounds for the proposal/initiative 2
1.4.1. Requirement(s) to be met in the short or long term including a detailed timeline for roll-out of the implementation of the initiative 2
1.4.2. 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. 2
1.4.3. Lessons learned from similar experiences in the past 3
1.4.4. Compatibility and possible synergy with other appropriate instruments 3
1.5. Duration and financial impact 4
1.6. Management mode(s) planned 4
2. MANAGEMENT MEASURES 6
2.1. Monitoring and reporting rules 6
2.2. Management and control system(s) 6
2.2.1. Justification of the management mode(s), the funding implementation mechanism(s), the payment modalities and the control strategy proposed 6
2.2.2. Information concerning the risks identified and the internal control system(s) set up to mitigate them 6
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) 6
2.3. Measures to prevent fraud and irregularities 6
3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE 7
3.1. Heading of the multiannual financial framework and new expenditure budget line(s) proposed 7
3.2. Estimated impact on expenditure 8
3.2.1. Summary of estimated impact on expenditure 8
3.2.2. Summary of estimated impact on appropriations of an administrative nature 11
3.2.3. Third-party contributions 13
3.3. Estimated impact on revenue 13

1. FRAMEWORK OF THE PROPOSAL/INITIATIVE

1.1. Title of the proposal/initiative

Proposal for a Directive concerning measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148

1.2. Policy area(s) concerned *(Programme cluster)*

Communications Networks, Content and Technology

1.3. The proposal/initiative relates to:

☐ **a new action**

☐ **a new action following a pilot project/preparatory action**[40]

☒ **the extension of an existing action**

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

1.4. Grounds for the proposal/initiative

1.4.1. 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 revision's objective is to increase the level of cyber resilience of a comprehensive set of businesses operating in the European Union across all relevant sectors, to reduce inconsistencies in the resilience across the internal market in the sectors already covered by the Directive and to improve the level of joint situational awareness and the collective capability to prepare and respond.

1.4.2. 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.

Cybersecurity resilience across the Union cannot be effective if approached in a disparate manner through national or regional silos. The NIS Directive came to address this shortcoming, by setting a framework for network and information systems security at national and Union levels. However, the first periodical review of the NIS Directive pointed to a number of inherent flaws, which have eventually led to considerable disparities across the Member States in terms of capabilities, planning and level of protection, which affect at the same time the level playing field for similar companies on the internal market.

The EU intervention going beyond the current measures of the NIS Directive is justified mainly by: (i) the cross-border nature of the problem; (ii) the potential of EU action to improve and facilitate effective national policies; (iii) the contribution of concerted and collaborative NIS policy actions to effective protection of data protection and privacy.

The stated objectives can hence be better achieved via EU level action, rather than by the Member States alone.

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

1.4.3. Lessons learned from similar experiences in the past

The NIS Directive is the first horizontal internal market instrument aimed at improving the resilience of networks and systems in the Union against cybersecurity risks. It has already contributed greatly to raising the common level of cybersecurity amongst the Member States. However, the review of the functioning and implementation of the Directive have pointed to a number of shortcomings, which, in addition to the growing digitalisation and need for more up-to-date response, have to be addressed in a revised legal act.

1.4.4. Compatibility and possible synergy with other appropriate instruments

The new proposal is fully consistent and coherent with other related initiatives such as the proposal for Regulation on Digital Operational Resilience for the financial Sector ("DORA") and the proposal for Directive on the resilience of critical operators of essential services. It is also consistent with the European Electronic Communication Code, the General Data Protection Regulation and the eIDAS Regulation.

The proposal is an essential part of the EU Security Union Strategy.

1.5. Duration and financial impact

☐ **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**

– Implementation with a start-up period from 2022 to 2025

– followed by full-scale operation.

1.6. Management mode(s) planned[41]

Direct management by the Commission

– ☒ 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;

– X☐ 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

The European Union Agency for Cybersecurity, ENISA, which has been granted a new permanent mandate by the Cybersecurity Act would assist the Member States and the Commission in the implementation of the revised NIS Directive.

As a result of the revised NIS Directive, as of 2022/23, ENISA will have additional action areas. While these action areas would be covered by ENISA's general tasks according to its mandate, they will result in additional workload for the agency. More precisely, in addition to its current action areas, under the Commission proposal for a revised NIS Directive ENISA will be required also to specifically incorporate into its work programme among others the

[41] 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

following actions: (i) to develop and maintain a European vulnerability registry (Article 6 (2) of the proposal), (ii) to provide the secretariat of the European Cyber Crises Liaison Organisation Network (CyCLONe), (Article 14 of the proposal) and to issue an annual report on the state of cybersecurity in the EU (Article 15 of the proposal), (iii) to support the organisation of peer reviews between Member States (Article 16 of the proposal), (iv) to collect aggregated incident data from Member States and issue technical guidance (Article 20 (9) of the proposal), (v) to create and maintain a registry for entities providing cross-border services (Article 25 of the proposal).

Therefore, a request for 5 supplementary FTEs will be made from 2022 with the corresponding budget about €0,61M per year to cover these new posts (see separate Financial Statement for agencies).

2. MANAGEMENT MEASURES

2.1. Monitoring and reporting rules

Specify frequency and conditions.

The Commission will periodically review the functioning of the Directive and report to the European Parliament and the Council, the first time three years after the entry into force. The Commission will also assess the correct transposition of the Directive by the Member States.

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

The unit within DG CNECT in charge of the policy field will manage the implementation of the Directive.

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

Very low risk, as the NIS Directive ecosystem is 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)

Not relevant. Only use of administrative budget (“Global envelope”).

2.3. Measures to prevent fraud and irregularities

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

Not relevant. Only use of administrative budget (“Global envelope”).

3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE

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

Heading of multiannual financial framework	Budget line	Type of expenditure	Contribution			
	Number [Heading…7……...……]	Diff./Non-diff.[42]	from EFTA countries[43]	from candidate countries[44]	from third countries	within the meaning of Article [21(2)(b)] of the Financial Regulation
	20 02 06 management expenditures 20 02 06	Non diff	NO	NO	NO	NO

[42] Diff. = Differentiated appropriations / Non-diff. = Non-differentiated appropriations.

[43] EFTA: European Free Trade Association.

[44] Candidate countries and, where applicable, potential candidates from the Western Balkans.

3.2. Estimated impact on expenditure

3.2.1. Summary of estimated impact on expenditure

EUR million (to three decimal places)

Heading of multiannual financial framework	**<…>**	[Heading……...……]

			2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	***Post 2027***	**TOTAL**
Operational appropriations (split according to the budget lines listed under 3.1)	Commitments	(1)									
	Payments	(2)									
Appropriations of an administrative nature financed from the envelope of the programme[45]	Commitments = Payments	(3)									
TOTAL appropriations for the envelope of the programme	Commitments	=1+3									
	Payments	=2+3									

Heading of multiannual financial framework	7	‘Administrative expenditure’ Meetings:Plenary meetings of the NIS Cooperation Group take place usually 4 times a year. The Commission covers costs related to catering and travel expenses of representatives of 27 Member States (one representative per MS). Costs of one meeting could reach up to €15K. Missions: Missions are releated to monitoring of the implementation of the NIS Directive. Example: In one year (May 2019- July 2020) we were supposed to organized so called 'NIS country visits' and visit all 27 MS in order to discuss

[45] 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.

		implementation of the NIS Directive across the EU.

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 , which is uploaded to DECIDE for interservice consultation purposes.

EUR million (to three decimal places)

		2021	2022	2023	2024	2025	2026	2027	*Post 2027*	TOTAL
Human resources		1,14	1,14	1,14	1,14	1,14	1,14	**1,14**		**7,98**
Other administrative expenditure		**0,09**	**0,09**	**0,09**	**0,09**	**0,09**	**0,09**	**0,09**		**0,63**
TOTAL appropriations under HEADING 7 of the multiannual financial framework	(Total commitments = Total payments)	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**		**8,61**

EUR million (to three decimal places)

		2021	2022	2023	2024	2025	2026	2027	*Post 2027*	TOTAL
TOTAL appropriations across HEADINGS of the multiannual financial framework	Commitments									
	Payments									

3.2.2. Summary of estimated impact on appropriations of an administrative nature

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

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

EUR million (to three decimal places)

Years	2021	2022	2023	2024	2025	2026	2027	TOTAL
HEADING 7 of the multiannual financial framework								
Human resources	1,14	1,14	1,14	1,14	1,14	1,14	**1,14**	**7,98**
Other administrative expenditure	0,09	0,09	0,09	0,09	0,09	0,09	**0,09**	**0,63**
Subtotal HEADING 7 of the multiannual financial framework	1,23	1,23	1,23	1,23	1,23	1,23	**1,23**	**8,61**

Outside HEADING 7[46] of the multiannual financial framework								
Human resources								
Other expenditure of an administrative nature								
Subtotal outside HEADING 7 of the multiannual financial framework								

TOTAL	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**8,61**

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.

46 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.

3.2.2.1. Estimated requirements of human resources

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

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

Estimate to be expressed in full time equivalent units

Years		2021	2022	2023	2024	2025	2026	2027
• Establishment plan posts (officials and temporary staff)								
Headquarters and Commission's Representation Offices		6	6	6	6	6	6	6
Delegations								
Research								
• External staff (in Full Time Equivalent unit: FTE) - AC, AL, END, INT and JED [47] Heading 7								
Financed from HEADING 7 of the multiannual financial framework	- at Headquarters	3	3	3	3	3	3	3
	- in Delegations							
Financed from the envelope of the programme [48]	- at Headquarters							
	- in Delegations							
Research								
Other (specify)								
TOTAL		**9**	**9**	**9**	**9**	**9**	**9**	**9**

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	• Preparation of delegated acts according to Article 18 (6), Article 21 (2), Article 36; • Preparation of implementing acts according to Article 12 (8), Article 18 (5), Article 20 (11); • Providing a Secretariat for the NIS Cooperation Group; • Organization of the NIS Cooperation Group's plenary meetings and work stream meetings; • Coordination of work of Member States on various documents (guidelines, toolboxes, etc.); • Liaison with other Commission services, ENISA and national authorities in view of implementing the NIS Directive; • Analysis of national methods and best practices related to the implementation of the NIS Directive.
External staff	Support to all above tasks as necessary

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

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

3.2.3. Third-party contributions

The proposal/initiative:

– X☐ does not provide for co-financing by third parties

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

Appropriations in EUR million (to three decimal places)

Years	2021	2022	2023	2024	2025	2026	2027	TOTAL
Specify the co-financing body								
TOTAL appropriations co-financed								

3.3. Estimated impact on revenue

– ☐X 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:	Impact of the proposal/initiative[49]						
	2021	2022	2023	2024	2025	2026	2027
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).

[49] 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.

ANNEX
to the LEGISLATIVE FINANCIAL STATEMENT

Name of the proposal/initiative:

Proposal for a Directive revising Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

……
……

1. NUMBER and COST of HUMAN RESOURCES CONSIDERED NECESSARY

2. COST of OTHER ADMINISTRATIVE EXPENDITURE

3. METHODS of CALCULATION USED for ESTIMATING COSTS

3.1 Human resources

3.2 Other administrative expenditure

*This annex, **to be completed by each DGs/Services participing to the proposal/initiative**, must accompany the legislative financial statement when the inter-services consultation is launched.*

The data tables are used as a source for the tables contained in the legislative financial statement. They are strictly for internal use within the Commission.

1. Cost of human resources considered necessary

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

X☐ The proposal/initiative requires the use of human resources, as explained below:

EUR million (to three decimal places)

HEADING 7 of the multiannual financial framework		2021		2022		2023		2024		2025		2026		2027		TOTAL	
		FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations
• Establishment plan posts (officials and temporary staff)																	
Headquarters and Commission's Representation Offices	AD	6	0.9	6	0.9	6	0.9	6	0.9	6	0.9	6	0.9	6	0.9	42	6,3
	AST																
in Union Delegations	AD																
	AST																
• External staff [50] 0.24																	
Global envelope	AC	3	0.24	3	0.24	3	0.24	3	0.24	3	0.24	3	0.24	3	0.24	21	1.68
	END																
	INT																
in Union Delegations	AC																
	AL																

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

	END																
	INT																
	JPD																
Other budget lines (*specify*)																	
Subtotal – HEADING 7 of the multiannual financial framework		9	1.14	9	1.14	9	1.14	9	1.14	9	1.14	9	1.14	9	1.14	63	7.98

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.

Outside HEADING 7 of the multiannual financial framework			2021		2022		2023		2024		2025		2025		2025		TOTAL	
			FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations
• Establishment plan posts (officials and temporary staff)																		
Research		AD																
		AST																
• External staff [51]																		
External staff from operational appropriations (former 'BA' lines).	- at Headquarters	AC																
		END																
		INT																
	- in Union delegations	AC																
		AL																
		END																
		INT																
		JPD																
Research)		AC																
		END																
		INT																

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

Other budget lines (*specify*)																	
Subtotal – Outside HEADING 7 of the multiannual financial framework																	

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.

Estimated impact on ENISA's human resources

The European Union Agency for Cybersecurity, ENISA, which has been granted a new permanent mandate by the Cybersecurity Act would assist the Member States and the Commission in the implementation of the revised NIS Directive.

As a result of the revised NIS Directive, as of 2022/23, ENISA will have additional action areas. While these action areas would be covered by ENISA's general tasks according to its mandate, they will result in additional workload for the agency. More precisely, in addition to its current action areas, under the Commission proposal for a revised NIS Directive ENISA will be required also to specifically incorporate into its work programme among others the following actions: (i) to develop and maintain a European vulnerability registry (Article 6 (2) of the proposal), (ii) to provide the secretariat of the European Cyber Crises Liaison Organisation Network (CyCLONe), (Article 14 of the proposal) and to issue an annual report on the state of cybersecurity in the EU (Article 15 of the proposal), (iii) to support the organisation of peer reviews between Member States (Article 16 of the proposal), (iv) to collect aggregated incident data from Member States and issue technical guidance (Article 20 (9) of the proposal), (v) to create and maintain a registry for entities providing cross-border services (Article 25 of the proposal).

Therefore, a request for 5 supplementary FTEs will be made from 2022 with the corresponding budget about €0,61M per year to cover these new posts (see separate Financial Statement for agencies).

Therefore, a request for 5 supplementary FTEs will be made from 2022 with the corresponding budget to cover these new posts.

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

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

EUR million (to three decimal places)

	Year **N** [52] **2022**	Year **N+1** **2023**	Year **N+2** **2024**	Year **N+3** **2025**	Enter as many years as necessary to show the duration of the impact (see point 1.6)			**TOTAL**
Temporary agents (AD Grades)	0.450	0.450	0.450	0.450	0.450	0.450		**2.7**

[52] 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.

Temporary agents (AST grades)								
Contract staff	0.160	0.160	0.160	0.160	0.160	0.160		
Seconded National Experts								**0.96**

TOTAL	**0.61**	**0.61**	**0.61**	**0.61**	**0.61**	**0.61**		**3.66**

Staff requirements (FTE):

	Year **N** [53] **2022**	Year **N+1** **2023**	Year **N+2** **2024**	Year **N+3** **2025**	Enter as many years as necessary to show the duration of the impact (see point 1.6)	**TOTAL**
Temporary agents (AD Grades)	3	3	3	3	3	3		**18**
Temporary agents (AST grades)								
Contract staff	2	2	2	2	2	2		**12**
Seconded National Experts								

[53] 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.

TOTAL	**5**	**5**	**5**	**5**	**5**	**5**		**30**

2. Cost of other administrative expenditure

☐ The proposal/initiative does not require the use of administrative appropriations
X☐ The proposal/initiative requires the use of administrative appropriations, as explained below:

EUR million (to three decimal places)

HEADING 7 of the multiannual financial framework	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Total**
At headquarters:								
Mission and representation expenses	0.03	0.03	0.03	0.03	0.03	0.03	0.03	**0.21**
Conference and meeting costs	0.06	0.06	0.06	0.06	0.06	0.06	0.06	**0.42**
Committees[54]								
Studies and consultations								
Information and management systems								
ICT equipment and services[55]								

[54] Specify the type of committee and the group to which it belongs.
[55] ICT: Information and Communication Technologies: DIGIT must be consulted.

Other budget lines (*specify where necessary*)								
In Union delegations								
Missions, conferences and representation expenses								
Further training of staff								
Acquisition, renting and related expenditure								
Equipment, furniture, supplies and services								
Subtotal HEADING 7 of the multiannual financial framework	0.09	0.09	0.09	0.09	0.09	0.09	0.09	**0.63**

EUR million (to three decimal places)

Outside HEADING 7 of the multiannual financial framework	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Total**
Expenditure on technical and administrative assistance (not including external staff) from operational appropriations (former 'BA' lines)								
- at Headquarters								
- in Union delegations								
Other management expenditure for research								
Other budget lines (*specify where necessary*)								
Sub-total – Outside HEADING 7 of the multiannual financial framework								

TOTAL HEADING 7 and Outside HEADING 7 of the multiannual financial framework	1.23	1,23	1,23	1,23	1,23	1,23	1,23	**8.61**

The administrative appropriations required will be met by the appropriations which are already assigned to management of the action and/or which have been redeployed, 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 existing budgetary constraints.

3. Methods of calculation used to estimate costs

3.1 Human resources

This part sets out the method of calculation used to estimate the human resources considered necessary (workload assumptions, including specific jobs (Sysper 2 work profiles), staff categories and the corresponding average costs)

HEADING 7 of the multiannual financial framework
NB: The average costs for each category of staff at Headquarters are available on BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/pre/legalbasis/Pages/pre-040-020_preparation.aspx
• Officials and temporary staff 6 FTE officials (average cost 0.150) = 0.9 by year - Preparation of delegated acts according to Article 18 (6), Article 21 (2), Article 36; - Preparation of implementing acts according to Article 12 (8), Article 18 (5), Article 20 (11); - Providing a Secretariat for the NIS Cooperation Group; - Organization of the NIS Cooperation Group's plenary meetings and work stream meetings; - Coordination of work of Member States on various documents (guidelines, toolboxes, etc.); - Liaison with other Commission services, ENISA and national authorities in view of implementing the NIS Directive; - Analysis of national methods and best practices related to the implementation of the NIS Directive.
• External staff 3 AC (average cost 0.08) = 0.24 by year - Support to all above tasks as necessary

Outside HEADING 7 of the multiannual financial framework
• Only posts financed from the research budget
• External staff

3.2 Other administrative expenditure

Give details of the method of calculation used for each budget line

and in particular the underlying assumptions (e.g. number of meetings per year, average costs, etc.)

HEADING 7 of the multiannual financial framework

Meetings: Plenary meetings of the NIS Cooperation Group take place usually 4 times a year. The Commission covers costs related to catering and travel expenses of representatives of 27 Member States (one representative per MS). Costs of one meeting could reach up to €15K, which gives €60K per year.

Missions: Missions are releated to monitoring of the implementation of the NIS Directive. Example: In one year (May 2019- July 2020) we were supposed to organized so called 'NIS country visits' and visit all 27 MS in order to discuss

implementation of the NIS Directive across the EU.

Outside HEADING 7 of the multiannual financial framework

ANNEX 7

to the
COMMISSION DECISION

on the Internal Rules on the implementation of the general budget of the European Union (European Commission section) for the attention of the Commission departments

LEGISLATIVE FINANCIAL STATEMENT 'AGENCIES'

This LFS covers the request to increase the staff of ENISA by 5 FTEs from 2022 to perform supplementary activities linked to the implementation of the NIS Directive. These activities are already covered by the ENISA mandate.

Contents

1. FRAMEWORK OF THE PROPOSAL/INITIATIVE 16
1.1. Title of the proposal/initiative 16
1.2. Policy area(s) concerned 16
1.3. The proposal relates to 16
1.4. Objective(s) 16
1.4.1. General objective(s) 16
1.4.2. Specific objective(s) 16
1.4.3. Expected result(s) and impact 18
1.4.4. Indicators of performance 18
1.5. Grounds for the proposal/initiative 19
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 19
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. 19
1.5.3. Lessons learned from similar experiences in the past 20
1.5.4. Compatibility with the Multiannual Financial Framework and possible synergies with other appropriate instruments 20
1.5.5. Assessment of the different available financing options, including scope for redeployment 20
1.6. Duration and financial impact of the proposal/initiative 21
1.7. Management mode(s) planned 21
2. MANAGEMENT MEASURES 23
2.1. Monitoring and reporting rules 23
2.2. Management and control system(s) 23
2.2.1. Justification of the management mode(s), the funding implementation mechanism(s), the payment modalities and the control strategy proposed 23
2.2.2. Information concerning the risks identified and the internal control system(s) set up to mitigate them 23
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) 23
2.3. Measures to prevent fraud and irregularities 24
3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE 24

3.1. Heading(s) of the multiannual financial framework and expenditure budget line(s) affected 24
3.2. Estimated impact on expenditure 26
3.2.1. Summary of estimated impact on expenditure 26
3.2.2. Estimated impact on [body]'s appropriations 28
3.2.3. Estimated impact on [body]'s human resources 29
3.2.4. Compatibility with the current multiannual financial framework 32
3.2.5. Third-party contributions 32
3.3. Estimated impact on revenue 33

1. FRAMEWORK OF THE PROPOSAL/INITIATIVE

1.1. Title of the proposal/initiative

Proposal for a Directive concerning measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148

1.2. Policy area(s) concerned

Communications Networks, Content and Technology

1.3. The proposal relates to

☐ **a new action**

☐ **a new action following a pilot project/preparatory action**[56]

☒ **the extension of an existing action**

☐ **a merger of one or more actions towards another/a new action**

1.4. Objective(s)

1.4.1. General objective(s)

The revision's objective is to increase the level of cyber resilience of a comprehensive set of businesses operating in the European Union across all relevant sectors, to reduce inconsistencies in the resilience across the internal market in the sectors already covered by the Directive and to improve the level of joint situational awareness and the collective capability to prepare and respond.

1.4.2. Specific objective(s)

In order to address the problem of low level of cyber resilience of businesses operating in the European Union, the specific objective is to ensure that entities in all sectors that are dependent on network and information systems and that provide key services to the economy and society as a whole are required to take cybersecurity measures and report incidents with a view to increasing the overall level of cyber resilience throughout the internal market.

In order to address the problem of inconsistent resilience across Member States and sectors, the specific objective is to ensure that all entities that are active in sectors covered by the NIS legal framework and that are similar in size and have a comparable role are subject to the same regulatory regime (are either inside or outside the scope) no matter under which jurisdiction they fall within the EU.

In order to ensure that all entities that are active in sectors covered by the NIS legal framework are required to follow the same obligations based on the concept of risk management when it comes to security measures and must report all incidents based on a uniform set of criteria, the specific objectives are to ensure that competent authorities enforce the rules laid down by the legal instrument more effectively through aligned supervisory and enforcement measures and to ensure a comparable level of resources across Member States allocated to competent authorities that would allow them to fulfil the core tasks laid out by the NIS framework.

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

In order to address the problem of joint situational awareness and lack of joint crisis response, the specific objective is to ensure that essential information is exchanged between Member States by introducing clear obligations for competent authorities to share information and cooperate when it comes to cyber threats and incidents and by developing a Union joint operational crisis response capacity.

1.4.3. Expected result(s) and impact

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

The proposal is expected to bring significant benefits: estimates indicate that it may lead to a reduction in cost of cybersecurity incidents by EUR 11.3 billion. The sectorial scope would be considerably enlarged under the NIS framework, but next to the above benefits, the burden that may be created by the NIS requirements, notably from the supervision perspective, would also be balanced for both the new entities to be covered and the competent authorities. This is because the new NIS framework would establish a two layer approach, with a focus on big and key entities and a differentiation of supervisory regime that allows only ex post supervision for a large number thereof, notably those considered 'important' yet not 'essential'.

Overall, the proposal would lead to efficient trade-offs and synergies, with the best potential out of all policy options analysed to ensure an increased and consistent level of cyber resilience of key entities across the Union that would eventually lead to cost savings for both businesses and society.

The proposal would also lead to certain compliance and enforcement costs for the relevant Member States authorities (an overall increase of about 20-30% of resources was estimated). However, the new framework would also bring substantial benefits through a better overview of and interaction with key businesses, enhanced cross-border operational cooperation, as well as mutual assistance and peer-review mechanisms. This would lead to an overall increase in cybersecurity capabilities across Member States.

For the companies that would fall under the scope of the NIS framework, it is estimated that they would need an increase of maximum 22% of their current ICT security spending for the first years following the introduction of the new NIS framework (this would be 12% for companies already under the scope of the current NIS Directive). However, this average increase of ICT security spending would lead to a proportionate benefit of such investments, notably due to a considerable reduction in cost of cybersecurity incidents (estimated to EUR 118 billion over ten years).

Small- and micro-businesses would be exempted from the scope of the NIS framework. For medium-sized enterprises, it can be expected that there would be an increase in the level of ICT security spending in the first years following the introduction of the new NIS framework. At the same time, raising the level of security requirements for these entities would also incentivise their cybersecurity capabilities and help improve their ICT risk management.

There would be an impact on national budgets and administrations: an estimated increase of approximately 20-30% of resources would be expected in the short and medium term.

No other significant negative impacts are expected. The proposal is expected to lead to more robust cybersecurity capabilities and consequently would have a more substantial mitigating impact on the number and severity of incidents, including data breaches. It is also likely to have a positive impact on ensuring a level playing field across Member States of all entities covered under the NIS scope and reduce cybersecurity information asymmetries.

1.4.4. Indicators of performance

Specify the indicators for monitoring progress and achievements.

The assessment of indicators will be conducted by the Commission, with the support of ENISA and the Cooperation Group, starting three years following the entry into force of the

new NIS legal act. Some of the monitoring indicators based on which the success of the NIS review would be assessed are as follows:

- Improved handling of incidents: By taking cybersecurity measures, companies are not only improving their ability to avoid certain incidents entirely, but also their incident response capacity. Measures of success are therefore i) the reduction of average time it takes to detect an incident, ii) the time it takes organisations on average to recover from an incident and iii) the average cost of a damage caused by an incident.

- Increased awareness of cybersecurity risks by the top management of companies: By requiring companies to take measures, a revised NIS Directive would contribute to raising awareness of cybersecurity related risks amongst the top management. This can be measured by studying to which extent companies under the NIS scope are prioritising cybersecurity in internal company policies and processes as evidenced by internal documentation, relevant training programmes and awareness activities for the employees and prioritising security-related ICT investment. The management of all essential and important entities should also be aware of the rules laid down by the NIS Directive.

- Levelling sector-specific spending: ICT security spending varies considerably between sectors in the EU. By requiring companies in more sectors to take measures, deviations from the average sector-specific ICT security spending as a percentage of overall ICT spending should diminish between sectors and across Member States.

- Stronger competent authorities and increased cooperation: A revised NIS Directive would potentially confer additional tasks on competent authorities. This would have a measurable impact on the financial and human resources dedicated to cybersecurity agencies at national level and should also have a positive impact on the capacity of competent authorities to proactively cooperate and therefore increase the number of cases where competent authorities are engaging with each other for the purpose of dealing with cross-border incidents or carrying out joint supervisory activities.

- Increased information sharing: The revised NIS would also improve information sharing among companies and with competent authorities. One of the targets of the review could be to increase the number of entities participating in the various forms of information sharing.

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 a comprehensive set of businesses operating in the European Union across all relevant sectors, to reduce inconsistencies in the resilience across the internal market in the sectors already covered by the Directive and to improve the level of joint situational awareness and the collective capability to prepare and respond. It will build on what has been achieved with the implementation of Directive (EU) 2016/1148 for the past 4 years.

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.

Cybersecurity resilience across the Union cannot be effective if approached in a disparate manner through national or regional silos. The NIS Directive came to address this

shortcoming, by setting a framework for network and information systems security at national and Union levels. However, the first periodical review of the NIS Directive pointed to a number of inherent flaws, which have eventually led to considerable disparities across the Member States in terms of capabilities, planning and level of protection, which affect at the same time the level playing field for similar companies on the internal market.

The EU intervention going beyond the current measures of the NIS Directive is justified mainly by: (i) the cross-border nature of the problem; (ii) the potential of EU action to improve and facilitate effective national policies; (iii) the contribution of concerted and collaborative NIS policy actions to effective protection of data protection and privacy.

The stated objectives can hence be better achieved via EU level action, rather than by the Member States alone.

1.5.3. Lessons learned from similar experiences in the past

The NIS Directive is 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 already contributed greatly to raising the common level of cybersecurity amongst the Member States. However, the review of the functioning and implementation of the Directive have pointed to a number of shortcomings, which, in addition to the growing digitalisation and need for more up-to-date response, have to be addressed in a revised legal act.

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

The new proposal is fully consistent and coherent with other related initiatives such as the proposal for Regulation on Digital Operational Resilience for the financial Sector ("DORA") and the proposal for Directive on the resilience of critical operators of essential services. It is also consistent with the European Electronic Communication Code, the General Data Protection Regulation and the eIDAS Regulation.

The proposal is an essential part of the EU Security Union Strategy.

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

The management of these tasks by ENISA necessitates specific profiles and supplementary workload which cannot be absorbed without any increase of human resources.

1.6. Duration and financial impact of the proposal/initiative

☐ **limited duration**

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

– ☐ Financial impact from YYYY to YYYY

☒ **unlimited duration**

– Implementation with a start-up period from 2022 to 2025,

– followed by full-scale operation.

1.7. Management mode(s) planned[57]

☒ **Direct management** by the Commission

through

– ☐ executive agencies

☐ **Shared management** with the Member States

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

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

☐the EIB and the European Investment Fund;

☒ bodies referred to in Articles 70 and 71;

☐ 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.

Comments

The European Union Agency for Cybersecurity, ENISA, which has been granted a new permanent mandate by the Cybersecurity Act would assist the Member States and the Commission in the implementation of the revised NIS Directive.

As a result of the revised NIS Directive, as of 2022/23, ENISA will have additional action areas. While these action areas would be covered by ENISA's general tasks according to its mandate, they will result in additional workload for the agency. More precisely, in addition to its current action areas, under the Commission proposal for a revised NIS Directive ENISA will be required also to specifically incorporate into its work programme among others the following actions: (i) to develop and maintain a European vulnerability registry (Article 6 (2) of the proposal), (ii) to provide the secretariat of the European Cyber Crises Liaison Organisation Network (CyCLONe), (Article 14 of the proposal) and to issue an annual report on the state of cybersecurity in the EU (Article 15 of the proposal), (iii) to

[57] 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.

support the organisation of peer reviews between Member States (Article 16 of the proposal), (iv) to collect aggregated incident data from Member States and issue technical guidance (Article 20 (9) of the proposal), (v) to create and maintain a registry for entities providing cross-border services (Article 25 of the proposal).

Therefore, a request for 5 supplementary FTEs will be made from 2022 with the corresponding budget about €0,61M per year to cover these new posts.

2. MANAGEMENT MEASURES

2.1. Monitoring and reporting rules

Specify frequency and conditions.

The Commission will periodically review the functioning of the Directive and report to the European Parliament and the Council, the first time three years after the entry into force.

The Commission will also assess the correct transposition of the Directive by the Member States.

The monitoring and reporting of the proposal will follow the principles outlined in ENISA's permanent mandate under REGULATION (EU) 2019/881 (Cybersecurity Act).

The data sources used for the planned monitoring would mostly be from ENISA, the Cooperation Group, the CSIRTs Network and the Member States' authorities. Besides the data gathered from the reports (including the annual activity reports) of ENISA, the Cooperation Group and the CSIRTs Network, specific data gathering tools could be used when needed (for example surveys to national authorities, Eurobarometer and reports from Cybersecurity Month campaign and the pan-European exercises).

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

The unit within DG CNECT in charge of the policy field will manage the implementation of the Directive.

As regards ENISA's management, Article 15 of the Cybersecurity Act provides a detailed list of the control functions of ENISA's Management Board.

Under Article 31 of the Cybersecurity Act, ENISA's Executive Director is responsible for the implementation of ENISA's budget and the Commission's internal auditor exercises the same powers over ENISA as over the Commission departments. ENISA's Management Board delivers an opinion on ENISA's final accounts.

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

Very low risk, as the NIS Directive ecosystem is already in place, and already covers ENISA, which has a permanent mandate following the entry into force of the Cybersecurity Act in 2019.

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)

The requested budgetary increase applies Title 1 and is intended to finance salaries. This means a very low risk of error at payment level.

2.3. Measures to prevent fraud and irregularities

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

The ENISA's prevention and protection measures would apply, specifically:

- Payments for any service or studies requested are checked by the agency's staff prior to payment, taking into account any contractual obligations, economic principles and good financial or management practice. Anti-fraud provisions (supervision, reporting requirements, etc.) will be included in all agreements and contracts concluded between the agency and recipients of any payments.

- 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 25 May 1999 concerning investigations conducted by the European Anti-fraud Office (OLAF) shall apply without restriction.

- Under Article 33 of the CSA, by 28 December 2019 ENISA acceded to the Inter-institutional Agreement of 25 May 1999 between the European Parliament and the Council of the European Union and the Commission of the European Communities concerning internal investigations by the European Anti-fraud Office (OLAF). ENISA shall issue, without delay, the appropriate provisions applicable to all the employees of the agency.

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.[58]	from EFTA countries [59]	from candidate countries[60]	from third countries	within the meaning of Article 21(2)(b) of the Financial Regulation
2	02 10 04	./Non-diff.	YES	NO	NO	/NO

- New budget lines requested

In order of multiannual financial framework headings and budget lines.

Heading of multiannual	Budget line	Type of expenditure	Contribution

[58] Diff. = Differentiated appropriations / Non-diff. = Non-differentiated appropriations.

[59] EFTA: European Free Trade Association.

[60] Candidate countries and, where applicable, potential candidates from the Western Balkans.

financial framework	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
	[XX.YY.YY.YY]		YES/NO	YES/NO	YES/NO	YES/NO

3.2. Estimated impact on expenditure

3.2.1. Summary of estimated impact on expenditure

EUR million (to three decimal places)

Heading of multiannual financial framework	Number	[Headin…2 Single Market, Innovation and Digital……..……]

[Body]: <…ENISA….>			Year **N**[61] **2022**	Year **N+1** **2023**	Year **N+2** **2024**	Year **N+3** **2025**	Enter as many years as necessary to show the duration of the impact (see point 1.6) **2026**	**2027**		**TOTAL**
Title 1:	Commitments	(1)	0.61	0.61	0.61	0.61	0.61	0.61		**3.66**
	Payments	(2)	0.61	0.61	0.61	0.61	0.61	0.61		**3.66**
Title 2:	Commitments	(1a)								
	Payments	(2a)								
Title 3:	Commitments	(3a)								
	Payments	(3b)								
TOTAL appropriations for [body] <ENISA…….>	Commitments	=1+1a +3a	0.61	0.61	O.61	0.61	0.61	0.61		**3.66**
	Payments	=2+2a +3b	0.61	0.61	0.61	0.61	0.61	0.61		**3.66**

61 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.

Heading of multiannual financial framework	5	'Administrative expenditure'

EUR million (to three decimal places)

		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
DG: <…….>									
• Human Resources									
• Other administrative expenditure									
TOTAL DG <…….>	Appropriations								

TOTAL appropriations under HEADING 5 of the multiannual financial framework	(Total commitments = Total payments)								

EUR million (to three decimal places)

		Year N[62] 2022	Year N+1 2023	Year N+2 2024	Year N+3 2025	Enter as many years as necessary to show the duration of the impact (see point 1.6) 2026	2027		TOTAL
TOTAL appropriations under HEADINGS 1 to 5 of the multiannual financial framework	Commitments	0.61	0.61	0.61	0.61	0.61	0.61		**3.66**
	Payments	0.61	0.61	0.61	0.61	0.61	0.61		**3.66**

62 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.

3.2.2. Estimated impact on [body]'s appropriations

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

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

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[63]	Average cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	Total No	Total cost
SPECIFIC OBJECTIVE No 1[64]…																		
- Output																		
- Output																		
- Output																		
Subtotal for specific objective No 1																		
SPECIFIC OBJECTIVE No 2 ...																		
- Output																		
Subtotal for specific objective No 2																		
TOTAL COST																		

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

64 As described in point 1.4.2. 'Specific objective(s)…'

3.2.3. Estimated impact on ENISA's human resources

3.2.3.1. Summary

As a result of the revised NIS Directive, as of 2022/23, ENISA will have additional tasks. While these tasks would be covered by ENISA's mandate, they will result in additional workload for the agency. More precisely, in addition to its current tasks, under the Commission proposal for a revised NIS Directive ENISA will be tasked among others (i) to develop and maintain a European vulnerability registry (Article 6 (2)), (ii) to provide the secretariat of the European Cyber Crises Liaison Organisation Network (CyCLONe), (Article 14) and to issue an annual report on the state of cybersecurity in the EU (Article 15), (iii) to support the organisation of peer reviews between Member States (Article 16), (iv) to collect aggregated incident data from Member States and issue technical guidance (Article 20 (9)), (v) to create and maintain a registry for entities providing cross-border services (Article 25).

Therefore, a request for 5 supplementary FTEs will be made from 2022 with the corresponding budget to cover these new posts.

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

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

EUR million (to three decimal places)

	Year **N** [65] **2022**	Year **N+1** **2023**	Year **N+2** **2024**	Year **N+3** **2025**	Enter as many years as necessary to show the duration of the impact (see point 1.6) **2026**	**2027**		**TOTAL**
Temporary agents (AD Grades)	0.450	0.450	0.450	0.450	0.450	0.450		**2.7**
Temporary agents (AST grades)								
Contract staff	0.160	0.160	0.160	0.160	0.160	0.160		**0.96**
Seconded National Experts								
TOTAL	**0.61**	**0.61**	**0.61**	**0.61**	**0.61**	**0.61**		**3.66**

Staff requirements (FTE):

[65] 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.

	Year N [66] 2022	Year N+1 2023	Year N+2 2024	Year N+3 2025	Enter as many years as necessary to show the duration of the impact (see point 1.6) 2026	2027		TOTAL
Temporary agents (AD Grades)	3	3	3	3	3	3		**18**
Temporary agents (AST grades)								
Contract staff	2	2	2	2	2	2		**12**
Seconded National Experts								
TOTAL	**5**	**5**	**5**	**5**	**5**	**5**		**30**

3.2.3.2. Estimated requirements of human resources for the parent DG

– ☐ 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 amounts (or at most to one decimal place)

	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)		
• **Establishment plan posts (officials and temporary staff)**							
XX 01 01 01 (Headquarters and Commission's Representation Offices)							
XX 01 01 02 (Delegations)							
XX 01 05 01 (Indirect research)							
10 01 05 01 (Direct research)							
• **External staff (in Full Time Equivalent unit: FTE)[67]**							

[66] 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.

XX 01 02 01 (AC, END, INT from the 'global envelope')								
XX 01 02 02 (AC, AL, END, INT and JPD in the Delegations)								
XX 01 04 *yy*[68]	- at Headquarters[69]							
	- in Delegations							
XX 01 05 02 (AC, END, INT – Indirect research)								
10 01 05 02 (AC, END, INT – Direct research)								
Other budget lines (specify)								
TOTAL								

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	
External staff	

Description of the calculation of cost for FTE units should be included in the Annex V, section 3.

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

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

69 Mainly for the Structural Funds, the European Agricultural Fund for Rural Development (EAFRD) and the European Fisheries Fund (EFF).

3.2.4. Compatibility with the current multiannual financial framework

– ☒ The proposal/initiative is compatible the current multiannual financial framework.

– ☐ The proposal/initiative will entail reprogramming of the relevant heading in the multiannual financial framework.

Explain what reprogramming is required, specifying the budget lines concerned and the corresponding amounts. The proposal is compatible with the 21/27 MFF. The offsetting of the budget requested to cover the increase of HR resources in ENISA will be done by reducing by the same amount the budget of the Digital Europe Programme (DEP) in the same Heading.

– ☐ The proposal/initiative requires application of the flexibility instrument or revision of the multiannual financial framework[70].

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.

– The proposal/initiative provides for the co-financing estimated below:

EUR million (to three decimal places)

	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
Specify the co-financing body								
TOTAL appropriations co-financed								

[70] See Articles 11 and 17 of Council Regulation (EU, Euratom) No 1311/2013 laying down the multiannual financial framework for the years 2014-2020.

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[71]						
		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 miscellaneous 'assigned' revenue, specify the budget expenditure line(s) affected.

Specify the method for calculating the impact on revenue.

[71] 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.