CHAMBER OF COMMERCE
OF THE
UNITED STATES OF AMERICA

VINCENT M. VOCI
EXECUTIVE DIRECTOR, POLICY AND OPERATIONS
CYBER, INTELLIGENCE, AND SUPPLY CHAIN
SECURITY DIVISION

ABEL TORRES
SENIOR DIRECTOR
CENTER FOR GLOBAL REGULATORY COOPERATION

April 1, 2020

Email: CNECT-H2@ec.europa.eu

Mr. Roberto Viola
Director General
Communications Networks, Content and Technology
European Commission
1049 Bruxelles/Brussel
Belgium

Subject: Cybersecurity – review of EU rules on the security of network and information systems

Dear Director General Viola:

The U.S. Chamber of Commerce welcomes the opportunity to provide comments on the European Commission's ("Commission" consultation of the revision of the Directive (EU) 2016/1148 concerning measures for a common, high-level of security of network and information systems across the Union ("NIS Directive" or "the Directive") aimed at fulfilling the Commission's requirements to review the functioning of the NIS Directive periodically.

The U.S. Chamber of Commerce ("Chamber") is the world's largest business federation, representing the interests of more than three million enterprises of all sizes and sectors. The Chamber is a longtime advocate for stronger commercial ties between the United States and the European Union. According to a recent Chamber study jointly commissioned with AmCham EU, the U.S. and EU are together responsible for over one-third of global gross domestic product, and transatlantic trade and investment supports 16 million jobs on both sides of the Atlantic. The Chamber is also a leading business voice on digital economy policy, including cybersecurity, artificial intelligence, data privacy, digital trade, and e-commerce. In the U.S. and globally, we advance sound policy frameworks that support economic growth, promote consumer protection, and foster innovation.

We want to emphasize five fundamental principles as the Commission evaluates the functioning of the NIS 2 Directive.

In a constantly evolving technological and threat landscape, the Chamber believes that the following recommendations will further strengthen the NIS 2 Directive.

1. Harmonization Across the Digital Single Market.
2. Cybersecurity Risk Management Measures.
3. Harmonize Incident Notification Requirements.
4. Leverage International Standards and Best Practices.
5. Commitment to Government and Important and Essential Entity Collaboration.

The Chamber strongly believes that risk management is foundational to adequate cybersecurity. We commend the Commission on imposing a cybersecurity risk management approach by providing a minimum list of security elements and requirements that must be applied. By introducing security requirements and setting baseline capabilities across the European Union, the Chamber appreciates the national security importance and positive outcomes associated with implementing the NIS 2 Directive. As the NIS 2 Directive develops, we recommend continuing a risk-based approach that relies on best practices to identify and protect against threats to important and essential services. Such an approach will foster innovation and reward security and innovation since the NIS 2 Directive will adapt to new technologies.

Private industry greatly benefits when governments incorporate existing cybersecurity frameworks, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework or the International Organization/International Electrotechnical Commission (ISO/IEC) 27001:2013, into any future policy enactments and avoid mandating national or regional approaches to standards and requirements that diverge from these international norms. Furthermore, the Chamber believes, to achieve greater harmonization and alignment a codified partnership between the EU Cooperation Group and important and essential entities on a wide range of issues, such as risk management measures, use of international standards and frameworks, and incident reporting requirement thresholds and timeframes needs to be realized. This will support efforts to alleviate divergent approaches that may only serve to fragment the digital single market.

The Chamber appreciates the Commission's willingness to consult with industry throughout the process. Public-private partnerships between important and essential entities and national competent authorities (i.e., ENISA and the CSIRTs Network) will support efforts to ensure that effective, transparent, accountable, and consultative processes are put in place. Our goal is to foster a more resilient ecosystem through the creation of industry-led, market-based cybersecurity solutions. We strongly believe that a multi-stakeholder approach to cybersecurity is the most effective way to encourage economic activity while ensuring the digital infrastructure's security.

The Chamber appreciates the opportunity to share with you our primary concerns with the Directive. We stand ready to work with the European Commission and key stakeholders, and industry in ongoing consultations regarding new policies and sound policy implementations associated with the Security of Network and Information Systems.

Thank you again for your time, and we look forward to a continuing dialogue that helps achieve Europe's goals for a high common level of cybersecurity across the Union. If you have any questions or clarify our positions, please contact Vince Voci (vvoci@uschamber.com) and Abel Torres (atorres@uschamber.com).

Sincerely,

Abel Torres
Senior Director
Center for Global Regulatory Cooperation
U.S. Chamber of Commerce

Vincent Voci
Executive Director
Cyber, Intelligence, and Supply Chain Security Division
U.S. Chamber of Commerce

Enclosure:
1. U.S. Chamber of Commerce Consultation on the revision of the NIS Directive Survey Responses

Cc: Khalil Rouhana, Jakub Boratynski

Enclosure:

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;
   (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) (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 Council29 [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.
4. This Directive applies without prejudice to Council Directive 2008/114/EC30 and Directives 2011/93/EU31 and 2013/40/EU32 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 harmonization

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;

(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 Council33;
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 Council34;
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 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 Council36;
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 Council37;
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);
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;
24. ‘essential entity’ means any entity of a type referred to as an essential entity in Annex I;
25. ‘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 Council38 [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 consultation with important and essential entities, in particular adopt the following policies:
   (a) a policy to enhance the security and resilience of important and critical entities and manage its cybersecurity risk;
   (b) 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;
   (c) guidelines regarding the inclusion and specification of cybersecurity-related requirements for ICT products and service in public procurement;
   (d) a policy to promote and facilitate coordinated vulnerability disclosure within the meaning of Article 6;
   (e) a policy related to sustaining the general availability and integrity of the public core of the open internet;
   (f) a policy to strengthen capacity to prevent interference by malicious actors aimed at undermining electoral process;
   (g) a policy on promoting and developing cybersecurity skills, awareness raising and research and development initiatives;
   (h) a policy on supporting academic and research institutions to develop cybersecurity tools and secure network infrastructure;

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

(j) 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.

(k) A policy for international collaboration an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation. The policy should enhance international coordination and communication on information sharing, capacity building, incident response, and standards alignment.

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.

COMMENTS AND JUSTIFICATION:

The Chamber recommends adding a requirement for national competent authorities to coordinate, communicate, collaborate, and consult with critical and important entities. National cyber strategies are most effective when integrating many pieces, parts, and authorities across public and private sectors. Cyberspace is a shared space. We encourage governments to combine our shared authorities, capabilities, and resources in the deepest and broadest ways to challenge adversaries who routinely crowdsource attacks on government and private sector entities. These need to be applied concurrently and integrated into a unity of effort rather than divisions of action. Public and private entities are encouraged to defend shared territory (i.e., cyberspace) jointly. Current national strategies that reflect detect and react measures are ineffective in the current threat landscape to match adversarial movements. Future policymaking should emphasize enhancing defense and resilience to national critical functions and missions, not necessarily the technologies that underpin those technologies.

National cyber strategies need to apply international relations to reflect cross-border critical and important entity dependency and cyber risk. The Chamber urges governments to break down the concepts of defending in patches and encourages deepening operational collaboration between public and private sectors.

While the Chamber appreciates that the Member States shall adopt and update national cyber strategies, these are critical capacity and confidence-building initiatives that set policy direction and organize public and private capability, capacity, and authorities. We are concerned that

national strategies will, in turn, generate a fragmented and uneven regulatory approach across the digital single market.

Article 6

Coordinated vulnerability disclosure and a European vulnerability registry

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 disclosures within the constructs of a European Union development framework for 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.

COMMENT (or JUSTIFICATION):

Security and resilience are crucial to the Chamber and are a priority for our members. Upon discovery, it is paramount to mitigate potential vulnerabilities according to their criticality, risk, and consequence. Our members have significant security vulnerability remediation experience. Any vulnerability disclosure process needs to fully incorporate the different perspectives and the operational and legal complexities associated with a diverse set of technology industry stakeholders, such as affected vendors(s), service provider(s), and vulnerability reporters, each with their own set of unique perspectives.

The Chamber encourages the Commission to work with the private sector to build on and not duplicate existing best practices and urges the Commission to facilitate industry-wide implementation of transparent policies for coordinated vulnerability disclosure. Governments, industry, and consumers benefit when existing standards, frameworks, and bests practices are leveraged as a starting point (e.g., International Organization /International Electrotechnical Commission ("ISO/IEC") DIS 30111 and ISO/IEC 29147, work of Global Forum on Cybersecurity Expertise, ICASI, and the U.S. Department of Homeland Security's CVD program) and incorporated into any future policy enactments..

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 Council39 [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 [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, risk

management, building capacity, frameworks and best practices, as well as standards and technical specifications alignment;

(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. Topics for discussion may include, but are not limited to the following:

i. identification of critical and important entities;
ii. alignment of cybersecurity risk management measures;
iii. alignment of incident reporting requirements;
iv. cybersecurity certification schemes; or
v. cybersecurity information sharing.

(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.

9. To further enhance the industry Cooperation Group communication, collaboration, and coordination in 4(j) there is established a Cooperation Group Industry Working Group, comprised of subject matter experts from essential and important entities. The Working Group shall meet with the Cooperation Group annual and then again on an as needed basis.

COMMENTS (or JUSTIFICATION):

The Cooperation Group has helped build capacity and share best practices across the Member States. The Chamber supports "organizing regular meetings with relevant private interested parties from across the Union to discuss activities carried out by the group to gather input on emerging policy challenges." We recognize that the NIS 2 Directive supports public-private cooperation; however, we encourage an expansion of cooperation and operational collaboration between essential and important entities. The Chamber also supports the Cooperation Group driving further alignment on standards, incident reporting, cybersecurity risk management, and frameworks and best practices.

The Chamber recommends that the Commission establish a NIS Industry Stakeholder Group to serve as an advisory group to the NIS Cooperation Group. Such an Industry Stakeholder Group should assist ENISA, the Member States, and the Commission to draft technical documents and provide evidence and experience in critical information infrastructure protection based on the experiences of covered entities. This group should consist of both important and essential entity representatives that fall under the NIS 2 Directive scope. The Chamber looks at the Stakeholder Cybersecurity Certification Group under Article 22 of the Cybersecurity Act as a model body for public-private collaboration.

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~~ may 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.~~
   - (h) Identify
     - i. Asset Management
     - ii. Business Environment
     - iii. Governance
     - iv. Risk Assessment
     - v. Risk Management Strategy
     - vi. Supply Chain Risk Management
   - (i) Protect
     - i. Identity Management, Authentication and Access Control

ii. Awareness and Training
iii. Data Security:
iv. Information Protection Processes and Procedures
v. Maintenance
vi. Protective Technology

(j) Detect
i. Anomalies and Events
ii. Security Continuous Monitoring
iii. Detection Processes

(k) Respond
i. Response Planning
ii. Communications
iii. Analysis
iv. Mitigation
v. Improvements

(l) Recover
i. Recovery Planning
ii. Communications

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.

COMMENTS (or JUSTIFICATION):

The Chamber strongly believes that risk management is foundational to effective cybersecurity. We applaud the Commission's strategic shift from security measures to cybersecurity risk management measures. As the directive develops, we recommend continuing a risk-based approach that relies on best practices to identify and protect against threats to important and essential entities. A risk-based approach, combined with detection, response, and recovery planning, aligns with an industry-supported, scalable, and international cyber risk management framework. To accomplish this, we believe that the NIS 2 directive should focus on assessing and identifying risk and methods for minimizing risk. Such an

approach will foster innovation and reward security and innovation since the directive will adapt to new technologies.

As such, the Chamber encourages NIS 2 Directive cybersecurity risk management measures to be based on the following**:**

1. Alignment with international standards (e.g., ISO/IEC 27001, ISO/IEC 27103) and frameworks (*e.g.*, NIST Framework for Improving Critical Infrastructure Cybersecurity) and industry best practices;
2. Reliance on market-driven mechanisms, risk-management based frameworks that are non-prescriptive and internationally aligned;
3. Measures rooted in public-private collaboration;
4. Flexible and adaptable approaches to encourage innovation;

While we agree that the use of encryption or enhanced cryptological tools are helpful for data protection, we urge that Commission be technology-neutral and not mandatory in requiring essential and important entities to use encryption. We further want to emphasize that the Commission should not add requirements to build in back doors, hand over encryption keys, restrict the use of encryption, or otherwise undermine encryption in any way, as such actions lead to insecurity.

Article 19

EU coordinated risk assessments of critical supply chains

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

COMMENT (or JUSTIFICATION):

Getting critical ICT service, system, or product security correct is a shared goal of the Chamber, industry, and the Commission. Reducing or mitigating the impact of ICT supply chain attacks would greatly benefit the EU, businesses, and citizens. However, it is not clear how the Commission and ENISA will carry out coordinated security risk assessments of specific critical ICT service, system, or product supply chains while considering technical and, where relevant, non-technical risk factors.

It is critical that governments account for the sophisticated and coordinated approach that foreign adversaries are pursuing to dominate the ICTS market – and act tactically in providing the necessary tools to help governments, their allies, and the business community compete in this new reality. We strongly urge the Commission to build multi-stakeholder engagement forums for joint industry and government collaboration.

We further recognize that governments are increasingly focusing on the security of supply chains. Within our government, we are tracking up to 30 different supply chain risk management activities. As the Commission looks internationally, we urge you to consider the work of the DHS Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force as an industry-supported framework. The Chamber believes it is a valuable instrument in collaborating on analysis and developing operational and policy recommendations for the ICT Supply Chain through its membership's collaborative efforts. For reference, members of the SCRM include 40 major information technology (IT) and communications companies, along with 20 federal agencies. The SCRM task force's four working groups relate to (1) information sharing, (2) threat assessments, (3) qualified bidders and qualified manufacturing lists, (4) counterfeit products, and (5) analysis of the COVID-19 pandemic on ICT supply chains. The SCRM Task Force offers a useful multi-stakeholder model for coordinated industry and government SCRM work.

The Commission must not place unrealistic expectations on the private sector when developing compliance or assessment programs associated with supply chains. Instead, the Commission should take steps to ensure public and private sector cooperation when identifying threats and creating appropriate solutions to maximize the impact on security and minimize the impact on business and trade. Similarly, coordinated risk assessments should not be targeted toward supply chains purely based on a country of origin.

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~~ 72 hours after having assessed an incident to meet the criteria in Article 20(3) shall make 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~~ year 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).

JUSTIFICATION: Currently, within the EU, several sectors and cross-sector cyber incident reporting requirements (e.g., the GDPR, the eIDAS Regulation, the NIS directive, the ECB SSM) set out different timeframes, taxonomies, and thresholds for reporting. We recommend a fully harmonized cyber incident reporting regime across all EU legislation and driven by ENISA and the EU Cyber Cooperation Group, in consultation with industry. Such a framework would provide significant benefits and efficiencies to essential and important entities, competent authorities, and CSIRTs.

We urge the proposals to enhance flexibility regarding the timing of reporting and further recommend at a minimum that the initial reporting timeline requirement be extended from 24 to 72 hours to bring into further alignment with GDPR. Also, reporting entities will have incomplete information with a 24-hour to 72-hour timeframe. For that reason, we recommend that reporting obligations should not commence until the reporting becomes necessary after an impacted entity determines it is a reportable incident, not when it is initially detected.

ENISA should work through the Cooperation Group and Member States' competent authorities to develop a standardized template for incident reporting. Such a template might include:

- Assessment tool for the impact of an incident on an organization's reputation.
- When to consider an outage has occurred, its geographic scope and number of customers affected.
- How to commonly assess incident severity?
- How to assess the financial losses and economic impact?

In developing the criteria for a reportable significant cyber incident, Member States should ensure that the thresholds established capture significant cyber threats and mitigate systemic risks. Fostering trusted information-sharing relationships between industry and government provides the richest dialogue for cybersecurity risk management. Mandatory incident reporting requirements should take care to avoid entities to over-notify competent authorities and CSIRTs with false positives or incidents that fall well below a serious and significant incident.

We would suggest that instead of focusing on forced reporting that this legislative proposal reorients towards building capability, capacity, communication, and coordination on the cyber incident response process rooted in trusted relationships with industry and backed by industry-supported best practices and frameworks (*e.g.*, Financial Stability Board Cyber Incident Response and Recovery Report) and international standards (*e.g.*, ISO 27035).

The proposal should also consider safeguards for organizations working with law enforcement on cybercrime investigations, and now disclosure to non-law enforcement authorities might impact malicious TTP. As this applies to Article 20(5), competent authorities and CSIRTs should grant flexibility to essential and important entities who can demonstrate during an ex-post audit that their cooperation with law enforcement was not intended to circumvent the obligations outlined in Article 20.

The legislation should grant additional flexibility to victim entities for providing a final incident report. In many instances, especially considering recent high-profile global cybersecurity exploits, final forensics reports took several months to compile and do not reflect a robust partnership between the victim entities and competent authorities on response and risk mitigation measures.

Section 20(9) seems to include a perfunctory reporting obligation for essential and important entities to structure and report all incident data to ENISA monthly, without any (a) requirements for ENISA to do anything with that incident information and share back with industry and (b) not be rooted in any sound cyber risk management practice. We urge the Commission to issue guidance on the cybersecurity purpose for its broad collection of incident data.

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 voluntarily 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, in coordination with industry, 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.

COMMENT (or JUSTIFICATION):

EU cybersecurity policies, procedures, and regulations should promote international alignment and interoperability with industry-backed approaches to risk management to the maximum extent possible. The Chamber encourages the Commission to leverage public-private partnerships to develop public policy by incorporating consensus-based standards, available accreditation schemes, and globally recognized practices to meet EU compliance interests. By working with the private sector, government agencies can promote transparency, leverage private sector resources, and contribute to economic and job growth.

As the Commission contemplates establishing a voluntary public-private framework for certification of products, services, and processes (i.e., certification schemes for 5G, cloud, etc.,) the Chamber strongly urges the Commission to:

1. Build on and not duplicate existing frameworks and best practices.
2. Promote the voluntary use of cybersecurity certification schemes.
3. Consider alternatives, appropriate to the risk profile, to third-party assessments like self-assessment, vendor attestations, or accreditation of third-party assessors as a means to build and maintain confidence in conformity assessment bodies.

The Chamber requests additional information regarding the relationship between NIS 2 and the Cybersecurity Act's specific legal framework. The Cybersecurity Act establishes an EU cybersecurity certification framework for ICT products, services, and processes. It is not clear how the national cybersecurity strategies that Member States are obligated to adopt interrelate with the broader EU cybersecurity strategy. In coordination with industry, every effort should be made by the Commission to avoid redundancy and overlap.

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, best practices, or frameworks 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.

COMMENT (or JUSTIFICATION):

It is critical to advance important standards policy to support open and competitive markets, particularly with emerging technology initiatives. The development of global (internationally accepted) standards in collaboration with the private sector is the best way to promote common approaches that are technically sound to deliver technology solutions and policy objectives. Such standards should be voluntary, open, transparent, globally recognized, consensus-based, and technology-neutral. This builds upon the international standards principals established by the World Trade Organization (WTO) Technical Barrier to Trade (TBT) agreement by promoting the alignment of standards across borders, facilitating trade in connected products, and stimulating innovation in industry.

We strongly encourage the European Commission and the Member States to leverage the multistakeholder approach to all internet policy issues. The multistakeholder model allows for adequate participation of a broader foundation of interested parties, including technical experts, industry, civil society, and governments. The multistakeholder model has driven outcomes leading to the rapid innovation of technologies, such as the internet, and has led to vast informational and societal benefits.

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.

COMMENT (or JUSTIFICATION):

The WHOIS database, maintained by ICANN, is a critical tool for discovering who is behind Internet websites. Information about the URL's actual owner is essential for law enforcement, intellectual property owners, investigators, and public safety officials combating online cybercrime and abuse. It is also a vital tool of the cybersecurity community's efforts to fight malware, botnets, and spam. As digital technologies continue to grow, the WHOIS is foundational to ensuring the stability and security of the global Internet. The Chamber strongly encourages the EU to validate and approve the usefulness of the WHOIS database as one of the key weapons in the fight against internet fraud and abuse.

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.

COMMENT AND JUSTIFICATION:

Cyber threat data sharing is a critical component of cybersecurity risk management. We applaud the Commission's legislative proposal for recognizing its importance and elevating the dialogue over information sharing, which is different and distinct from incident or breach notification protocols and procedures. It is essential to underscore that information exchange is based on trust, which is incredibly difficult to regulate and requires a sustained and persistent commitment on behalf of recipients and contributors to maintain.

The Chamber recommends that the Commission add additional clarity to the types of information authorized to be exchanged. For example, businesses routinely share at machine speed the following types of structured data: indicators of compromise, signatures, hashes, internet protocol addresses, emails to enhance the level of cybersecurity. We seek clarity on whether these specific types of data are exempt from Regulation (EU) 2016/679 and urge the Commission to be as detailed as possible to ensure that for certain cybersecurity activities, this information is protected.

Also, the Chamber recommends that the Commission urge the Member States to consider incentive packages for important and essential entities to participate in an information-sharing program voluntarily, whether that's a part of an information sharing and analysis center (or organization) or another sharing entity (e.g., Cyber Threat Alliance) or contract with a private sector cyber threat intelligence company. Potential incentives may include tax incentives, direct subsidies, protections from liability, antitrust, or disclosure.

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;

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