SUBSIDIARY LEGISLATION 460.41

MEASURES FOR A HIGH COMMON LEVEL OF CYBERSECURITY ACROSS THE EUROPEAN UNION (MALTA) ORDER

23rd January, 2026

LEGAL NOTICE 71 of 2025.

PART I - PRELIMINARY

Citation and scope.

1. (1) The title of this order is Measures for a High Common Level of Cybersecurity across the European Union (Malta) Order.

(2) The scope of this order is to transpose Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

Interpretation.

2. (1) In this order unless the context otherwise requires:

"Advisory Board" means the Critical Infrastructure Protection Advisory Board established by virtue of article 5;

"autonomous CSIRT" means an outsourced CSIRT which provides a monitoring function of CSIRT services to essential or important entities;

"background check" means a background check as defined in Directive (EU) 2022/2557;

"Charter" means the Charter of Fundamental Rights of the European Union;

"CIP Department" means the Critical Infrastructure Protection Department as established by virtue of article 7;

"cloud computing service" means a digital service that enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources, including where such resources are distributed across several locations. For the purposes of this definition:

(i) computing resources shall include resources such as networks, servers or other infrastructure, operating systems, software, storage,

applications and services. The service models of cloud computing include, *inter alia*, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS) and Network as a Service (NaaS). The deployment models of cloud computing shall include private, community, public and hybrid cloud;

(ii) the cloud computing service and deployment models shall have the same meaning as the terms of service and deployment models defined under ISO/IEC 17788:2014 standard;

(iii) the capability of the cloud computing user to unilaterally self-provision computing capabilities, such as server time or network storage, without any human interaction by the cloud computing service provider may be described as on-demand administration;

(iv) the term "broad remote access" is used to describe that the cloud capabilities are provided over the network and accessed through mechanisms promoting use of heterogeneous thin or thick client platforms, including mobile phones, tablets, laptops and workstations;

(v) the term "scalable" refers to computing resources that are flexibly allocated by the cloud service provider, irrespective of the geographical location of the resources, in order for the resources provided to handle fluctuations in demand;

(vi) the term "elastic pool" is used to describe computing resources that are provided and released according to demand in order to rapidly increase and decrease resources available depending on workload.

(vii) the term "shareable" is used to describe computing resources that are provided to multiple users who share a common access to the service, but where the processing is carried out separately for each user, although the service is provided from the same electronic equipment;

(viii) the term "distributed" is used to describe computing resources that are located on different networked computers or devices and which communicate and coordinate among themselves by message passing;

"Commission Recommendation 2003/361/EC" means the Commission Recommendation of 6 May 2003 concerning the

definition of micro, small and medium-sized enterprises;

"competent authority" means the Critical Infrastructure Protection Department or any authority as may from time to time be designated by the Prime Minister under article 7;

"consumer" means a consumer as defined in article 2 of the Consumer Affairs Act; Cap. 378.

"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;

"Cooperation Group" means the Cooperation Group established in accordance with Article 14 of Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive);

"coordinated vulnerability disclosure" means a structured process through which potential vulnerabilities pertaining to ICT products, ICT processes or ICT services could be identified and reported to the entity. Coordinated vulnerability disclosure also includes coordination between the reporting natural or legal person and the entity of the potentially vulnerable ICT products, ICT processes or ICT services;

"critical information infrastructure" or "CII" means an information and communication technology assets, systems, networks or part thereof which are essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in Malta as a result of the failure to maintain those functions;

"critical infrastructure" or "CI" has the same meaning assigned to it in Directive (EU) 2022/2557;

"CSIRT" means a computer security incident response team designated or established in accordance with articles 8 to 10;

"CSIRTs network" means the network of national CSIRTs established in accordance with Article 15 of the Directive;

"cyber threat" means a cyber threat as defined in Article 2(8) of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act);

"cybersecurity" means cybersecurity as defined in Article 2(1) of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act);

"data centre service" means a service that encompasses structures, or groups of structures, dedicated to the centralised accommodation, interconnection and operation of IT and network equipment providing data storage, processing and transport services together with all the facilities and infrastructures for power distribution and environmental control, and shall not apply to in-house corporate data centres owned and operated by the entity concerned for its own purpose;

"Director" means the Director, Critical Infrastructure Protection Department;

"DNS service provider" means an entity that provides:

(a) publicly available recursive domain name resolution services for internet end-users; or

(b) authoritative domain name resolution services for third-party use, with the exception of root name servers;

"Directive (EU) 2022/2555" means Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive);

"Directive (EU) 2022/2557 means Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC;

"domain name system" or "DNS" means a hierarchical distributed naming system which enables the identification of

internet services and resources, allowing end-user devices to use internet routing and connectivity services to reach those services and resources;

"electronic communications service" means an electronic communications service as defined in article 2 of the Electronic Communications (Regulation) Act; Cap. 399.

"ENISA" means the European Union Agency for Cybersecurity established in accordance with Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act);

"entity" means a 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;

"entity providing domain name registration services" means a registrar or an agent acting on behalf of registrars, such as a privacy or proxy registration service provider or reseller;

"ICT process" means an ICT process as defined in Article 2(14) of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act);

"ICT product" means an ICT product as defined in Article 2(12) of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act);

"ICT service" means an ICT service as defined in Article 2(13) of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act);

"incident" means an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via,

network and information systems;

"incident handling" means any actions and procedures aimed at preventing, detecting, analysing, and containing or responding to and recovering from it;

Cap. 586.

"Information and Data Protection Commissioner" means the Information and Data Protection Commissioner as appointed in accordance with article 11 of the Data Protection Act;

"internal CSIRT" means an internal CSIRT that operates within the structure of an entity to which it provides CSIRT monitoring services;

"internet exchange point" means a network facility which enables the interconnection of more than two (2) independent networks or autonomous systems, primarily for the purpose of facilitating the exchange of internet traffic, which provides interconnection only for autonomous systems and which neither requires the internet traffic passing between any pair of participating autonomous systems to pass through any third autonomous system nor alters or otherwise interferes with such traffic;

"large-scale cybersecurity incident" means an incident which causes a level of disruption that exceeds a Member State's capacity to respond to it or which has a significant impact on at least two (2) Member States;

"legitimate access seekers" means any person making a lawful and duly substantiated request for access to domain name registration services in accordance with national and Union law. They can include the CIP Department or where designated the competent authority in accordance with this order and those that are competent under national law or Union law for the prevention, investigation, detection or prosecution of criminal offences, and CERTs or CSIRTs;

"managed security service provider" means a managed service provider that carries out or provides assistance for activities relating to cybersecurity risk management;

"managed service provider" means an entity that provides services related to the installation, management, operation or maintenance of ICT products, networks, infrastructure and applications or any other network and information systems, via assistance or active administration carried out either on customers' premises or remotely;

"management body" shall include the head of the essential and important entity and any other officers appointed by the head for the purpose of carrying out article 18(1);

"Minister" means the Minister responsible for critical infrastructure protection;

"National Cyber Security Steering Committee" means the Malta Information and Technology Agency;

"national cybersecurity strategy" means a coherent framework providing strategic objectives and priorities in the area of cybersecurity and the governance to achieve them at national level;

"near miss" means an event that may have compromised the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via network and information systems, but that was successfully prevented from materialising or that did not materialise;

"network and information system" means:

(a) an electronic communications network as defined in article 2 of the Electronic Communications (Regulation) Act; Cap. 399.

(b) any device or group of interconnected or related devices, one (1) or more of which, pursuant to a programme, carry out automatic processing of digital data; or

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

"online marketplace" means an online marketplace as defined in article 51A of the Consumer Affairs Act; Cap. 378.

"online search engine" means an online search engine as defined in Article 2(5) of Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services;

"operator security plan" means the overall procedure identifying the assets, systems, networks or part thereof within critical information infrastructures, essential and important

entities, identifying the security solutions and technical measures that exist or are being implemented for their protection and the identification, selection and prioritisation;

"peer review" means the exercise organised in accordance with Article 19 of the Directive;

Cap. 249.

"person" means a person as defined in article 4 of the Interpretation Act;

"protocol on the sharing of information (Traffic Light Protocol)" means a protocol on the sharing of information (Traffic Light Protocol) which is a means of providing information on any limitations regarding the further dissemination of the same information;

"public administration entity" means an entity recognised as such in accordance with national law, not including the judiciary, the Parliament of Malta or the Central Bank of Malta, which complies with the following criteria:

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

(b) it has legal personality or is entitled by law to act on behalf of another entity with legal personality;

(c) it is financed, for the most part, by the State,

or by other bodies governed by public law, and is subject to management supervision by those authorities or bodies, or has an administrative, managerial or supervisory board, more than half of whose members are appointed by the State, or by other bodies governed by public law; and

(d) it has the power to address administrative or regulatory decisions to natural or juridical persons which affect their rights in the cross-border movement of persons, goods, services or capital;

"public electronic communications network" means a public electronic communications network as defined in article 2 of the Electronic Communications (Regulation) Act;

Cap. 399.

"qualified auditor" means a person who satisfies the requirements in accordance with article 14;

"qualified trust service" means a qualified trust service as

defined in Article 3(17) of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC;

"qualified trust service provider" means a qualified trust service provider as defined in Article 3(20) of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC;

"Regional Committees" shall have the same meaning assigned to it in accordance with the Regional Committees Regulations; S.L. 363.160.

"representative" means a natural or juridical person established in the Union explicitly designated to act on behalf of a DNS service provider, a TLD name registry, an entity providing domain name registration services, a cloud computing service provider, a data centre service provider, a content delivery network provider, a managed service provider, a managed security service provider, or a provider of an online marketplace, of an online search engine or of a social networking services platform that is not established in the Union, which may be addressed by the CIP Department or where designated the competent authority or CSIRT in the place of the entity itself with regard to the obligations of such entity in accordance with this order;

"research organisation" means an entity which has as its primary goal to conduct applied research or experimental development with a view to exploiting the results of such research for commercial purposes, but which does not include educational institutions;

"risk" means the potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of the incident;

"risk assessment" means the overall process of risk identification, risk analysis and risk evaluation, incorporating the identification of risk sources, events, their causes and their potential consequences, comprehending the nature of risk and determining the level of risk, with the ultimate objective of comparing the results of the risk analysis with the risk criteria in order to determine whether the risk and, or its magnitude is

acceptable or tolerable;

"security of network and information systems" means the ability of network and information systems to resist, at a given level of confidence, any event that may compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible by means of those network and information systems;

S.L. 419.06.

"service" means a service as defined in regulation 2 of the Notification Procedure Regulations;

"single point of contact" means the CIP Department established by virtue of article 7;

"significant cyber threat" means a cyber threat which, based on its technical characteristics, may be assumed to have the potential to have a severe impact on the network and information systems of an entity or the users of the entity's services by causing considerable material or non-material damage;

"significant incident" means an incident which:

(a) has caused or is capable of causing severe operational disruption of the service or financial loss for the entity concerned; or

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

"social networking services platform" means a platform that enables end-users to connect, share, discover and communicate with each other across multiple devices, in particular by means of chats, posts, videos and recommendations;

"standard" means a standard as defined in Article 2(1) of Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council;

"technical specification" means a technical specification

as defined in Article 2(4) of Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council;

"top-level domain name registry" or "TLD 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, irrespective of whether any of those operations are carried out by the entity itself or are outsourced, but excluding situations where TLD names are used by a registry only for its own use;

"trader" means any natural or juridical person, who is acting, including through any person acting in his name or on his behalf, for purposes relating to his trade, business, craft or profession;

"Tribunal" means the Administrative Review Tribunal established by article 5(1) under the Administrative Justice Act; Cap. 490.

"trust service" means a trust service as defined in Article 3(16) of the Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework;

"trust service provider" means a trust service provider as defined in Article 3(19) of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, as regards establishing the European Digital Identity Framework;

"vulnerability" means a weakness, susceptibility or flaw of ICT products or ICT services that may be exploited by a cyber threat;

"Union" means the European Union.

(2) Unless the context otherwise requires, words and phrases used in this order which are not defined herein, shall have the same meaning as assigned to them in the Directive.

Applicability.

3. (1) This order applies to public or private entities of a type listed in the First or Second Schedule which qualify as medium-sized enterprises under Article 2 of the Annex of Commission Recommendation 2003/361/EC or exceed the ceilings for medium-sized enterprises provided for in that article, and which provide their services or carry out their activities within the Union.

(2) Article 3(4) of the Annex to Commission Recommendation 2003/361/EC shall not apply for the purposes of this order.

(3) Regardless of their size, this order also applies to entities of a type listed in the First or Second Schedule, where:

(a) services are provided by:

(i) providers of public electronic communications networks or of publicly available electronic communications services;

(ii) trust service providers;

(iii) top-level domain name registries and domain name system service providers;

(b) the entity is the sole provider in Malta of a service which is essential for the maintenance of critical societal or economic activities;

(c) disruption of the service provided by the entity may have a significant impact on public safety, public security or public health;

(d) disruption of the service provided by the entity may induce a significant systemic risk, in particular for sectors where such disruption may have a cross-border impact;

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

(f) the entity is a public administration entity:

(i) if it is a government entity established in accordance with national law; or

(ii) if it is a local government authority established in accordance with national law and which following a risk assessment, provides services the disruption of which may have a significant impact on critical or societal or economic activities.

(4) Regardless of their size, this order applies to entities identified as critical entities in accordance with Directive (EU) 2022/2557;

(5) Regardless of their size, this order also applies to entities providing domain name registration services.

(6) This order is without prejudice to Malta's responsibility for safeguarding its national security and its power to safeguard other essential State functions, including ensuring the territorial integrity of the State and maintaining law and order.

(7) This order shall not apply to public administration entities that carry out their activities in the areas of national security, public security, defence or law enforcement, including the prevention, investigation, detection and prosecution of criminal offences.

(8) Entities which carry out activities in the areas of national security, public security, defence or law enforcement, including the prevention, investigation, detection and prosecution of criminal offences, or which provide services exclusively to the public administration entities referred to in sub-article (7) are exempt from the obligations laid down in articles 19 or 20 with regard to those activities or services. The supervisory and enforcement measures in Part VII shall not apply in relation to those specific activities or services:

Provided that where the entities carry out activities or provide services exclusively of the type in this sub-article, those entities shall also be exempt from the obligations established in article 24.

(9) Sub-articles (7) and (8) shall not apply where an entity acts as a trust service provider.

(10) This order shall not apply to entities which are exempted from the scope of Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011, in accordance with Article 2(4) of the said Regulation.

(11) The obligations established in this order shall not entail the supply of information the disclosure of which would be contrary to the essential interests of the national security, public security or defence of Malta.

Cap. 586.
S.L. 586.01.
Cap. 9.

(12) This order applies without prejudice to the Data Protection Act, the Processing of Personal Data (Electronic Communications Sector) Regulations, the Criminal Code and Directive (EU) 2022/2557;

(13) Without prejudice to Article 346 of the Treaty on the Functioning of the European Union, information that is confidential pursuant to Union or national rules, such as rules on business confidentiality, shall be exchanged with the European Commission and other relevant authorities in accordance with this order only where that exchange is necessary for the application of this order. The information exchanged shall be limited to that which is relevant and proportionate to the purpose of such exchange. The exchange of information shall preserve the confidentiality of such information and protect the security and commercial interests of entities concerned.

(14) Entities, the CIP Department or where designated the competent authority, the single point of contact and CSIRTs shall process personal data to the extent necessary for the purposes of this order and in accordance with the Data Protection Act, including the regulations made thereunder, and Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), in particular such processing shall rely on Article 6 of the said Regulation.

Cap. 586.

(15) The processing of personal data pursuant to this order by providers of public electronic communications networks or providers of publicly available electronic communications services shall be carried out in conformity with national data protection legislation, Union data protection law and Union privacy law, in particular the Processing of Personal Data (Electronic Communications Sector) Regulations.

S.L. 586.01.

(16) Where sector-specific Union legal acts require essential or important entities to adopt cybersecurity risk-management measures or to notify the CSIRT of significant incidents and where those requirements are at least equivalent in effect to the obligations established in this order, the relevant provisions of this order, including the provisions on supervision and enforcement established in Part VII, shall not apply to such entities:

Provided that where sector-specific Union legal acts do

not cover all entities in a specific sector falling within the scope of this order, the relevant provisions of this order shall continue to apply to the entities not covered by those sector-specific Union legal acts.

(17) The requirements in sub-article (16) shall be considered to be equivalent in effect to the obligations established in this order where:

(a) the cybersecurity risk-management measures are at least equivalent in effect to those in articles 19(1), (2) and (3); or

(b) the sector-specific Union legal act provides for immediate access, where appropriate automatic and direct, to the incident notifications by CSIRT by the CIP Department or where designated the competent authority or the single points of contact in accordance with this order and where requirements to notify significant incidents are at least equivalent in effect to those established in articles 20(1) to (6).

Essential and important entities.

4. (1) For the purposes of this order, the following entities shall be considered to be essential entities:

(a) entities of a type indicated in the First Schedule which exceed the ceilings for medium-sized enterprises provided for in accordance with Article 2(1) of the Annex to the Commission Recommendation 2003/361/EC;

(b) qualified trust service providers and top-level domain name registries as well as DNS service providers, regardless of their size;

(c) providers of public electronic communications networks or of publicly available electronic communications services which qualify as medium-sized enterprises in accordance with Article 2 of the Annex to the Commissioner Recommendation 2003/361/EC;

(d) public administration entities mentioned in article 3(3)(f)(i);

(e) any other entity of a type referred to in the First or Second Schedule that are identified by the CIP Department or where designated the competent authority as an essential entity pursuant to articles 3(3)(b) to (e);

(f) entities identified as critical entities under the Resilience of Critical Entities and Infrastructures (Identification, Designation and Protection) Order in article 3(4);

(g) entities which the CIP Department or where designated the competent authority identified before 16 January 2023 as operators of essential services in conformity with:

(i) Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive); or

(ii) national law.

(2) For the purposes of this order, entities of a type referred to in the First or Second Schedule which do not qualify as essential entities pursuant to sub-article (1) shall be considered to be important entities. This includes entities identified by the CIP Department or where designated the competent authority as important entities pursuant to articles 3(3)(b) to (e).

PART II – CRITICAL INFRASTRUCTURE PROTECTION ADVISORY BOARD, CRITICAL INFRASTRUCTURE PROTECTION DEPARTMENT AND CSIRT

Critical Infrastructure Protection Advisory Board.

5. (1) There shall be a Board to be known as the Critical Infrastructure Protection Advisory Board hereinafter referred to as "the Advisory Board", composed of such members of known integrity as shall be appointed by the Minister.

(2) The Advisory Board shall be composed of three (3) voting members including a Chairperson and a secretary who shall be appointed by the Minister for a term of three (3) years as follows:

(a) a lawyer who shall act as Chairperson to the Advisory Board;

(b) one (1) person with experience or qualifications in matters concerning critical infrastructure protection or related areas;

(c) one (1) person with experience or qualifications in matters concerning critical infrastructure protection or related areas; and

(d) a secretary who shall be a public official from within the ministry responsible for critical infrastructure protection, but who shall not have any voting rights:

Provided that a lawyer shall not be qualified to act as a Chairperson to the Advisory Board unless he has practised as an

advocate in Malta for a period of, or periods amounting in the aggregate to, not less than seven (7) years:

Provided further that a person appointed in terms of paragraphs (b) and (c) shall have at least four (4) years of experience:

Provided further that the members of the Advisory Board shall be in possession of a background check issued by the competent authority in accordance with Directive (EU) 2022/2557;

(3) The members of the Advisory Board shall be eligible for reappointment for subsequent terms of three (3) years:

Provided that the Advisory Board shall continue to exercise its functions until new members are appointed.

(4) If any vacancy in the Advisory Board occurs during the period of appointment, on account of death, resignation or for any other cause, the Minister shall, as soon as practicable, appoint another person to fill the vacancy:

Provided that the Advisory Board and the members thereof may act notwithstanding any such vacancy.

(5) The quorum of the Advisory Board shall consist of the Chairperson and not less than half of the members who are eligible to vote.

(6) The Chairperson shall have an original vote and where the votes are equally divided, a second or casting vote.

(7) One of the members of the Advisory Board shall act as chairperson in the absence of the Chairperson.

(8) Notwithstanding any other provision of this article, the Minister may at any time terminate the appointment of an appointed member if, in his opinion, such appointed member is unfit to continue in office or has become incapable of properly performing his functions.

(9) The Advisory Board shall communicate to the CIP Department, a copy of its recommendations and the relative deliberations leading to its recommendations, as soon as practicable:

Provided that the recommendation shall be communicated within ninety (90) days:

Provided further that in urgent cases, the Director may request the Advisory Board to issue its recommendations within thirty (30) days.

(10) The Chairperson may require the Director to be present at the Advisory Board meetings and to provide information as necessary.

(11) The Advisory Board may engage such consultants, as it may consider necessary to assist it in the fulfilment of its functions.

(12) The Advisory Board shall regulate its own procedures.

Function of the Advisory Board.

6. The Advisory Board shall issue recommendations and give its advice to the CIP Department in relation to the imposition of an administrative penalty in accordance with article 32.

Critical Infrastructure Protection Department.

7. (1) The CIP Department shall be the national supervisory authority responsible for monitoring the implementation of this order at national level and ensuring compliance therewith, implementing relevant provisions of this order and covering the sectors, sub-sectors and types of entities listed in the First and Second Schedule:

Provided that the CIP Department may make recommendations to the Prime Minister for the designation of competent authorities, in consultation with the Minister responsible for critical infrastructure protection and the Minister responsible for the sector, sub-sector or type of entity listed in the First or Second Schedule, which authorities shall be empowered to exercise such functions, obligations and powers given to them under this order, and shall satisfy all the requirements imposed on competent authorities by this order:

Provided further that the Malta Communications Authority shall be the competent authority in relation to the following sectors:

(a) for the following areas within the Digital Infrastructure sector as identified in the First Schedule:

(i) providers of public electronic communications networks;

(ii) providers of publicly available electronic communications services; and

(iii) trust service providers.

(b) for the postal and courier services sector as identified in the Second Schedule:

(i) postal service providers as defined in Article 2, point (1a) of Directive 97/67/EC of the European Parliament and of the Council of 15 December

1997 on common rules for the development of the internal market of Community postal services and the improvement of quality of service, including providers of courier services.

(2) Unless otherwise expressly provided in this order or any other law, and unless another designated competent authority is responsible for the sector, sub-sector or type of entity in the First or Second Schedule, the CIP Department shall be responsible for:

(a) establishing the criteria for the identification and designation of essential and important entities;

(b) identifying and designating essential and important entities;

(c) identifying the services provided by essential and important entities;

(d) ensuring that risk assessments are carried out by essential and important entities;

(e) ensuring that operator security plans and business continuity plans are drawn up and maintained by essential and important entities;

(f) instigating simulated runs of operator security plans and business continuity plans by essential and important entities;

(g) building partnerships with operators of Critical Information Infrastructures (CIIs) for information sharing, without prejudice to article 26;

(h) establishing a national self-registration mechanism for essential and important entities providing services in Malta, the CSIRTs providing monitoring services within such entities as well as entities providing domain name registration services in Malta, which shall provide information in accordance with article 24(1);

(i) establishing a register on the basis of paragraph (h) by 30 October 2025 and reviewing and, where appropriate, updating such register on a regular basis and at least every two (2) years;

(j) adopting a strategy on the security of network and information systems, under the national cybersecurity strategy in accordance with article 15;

(k) monitoring cybersecurity risk-management measures undertaken by essential and important entities in accordance with article 19;

(l) monitoring reporting obligations undertaken by essential and important entities in accordance with article 20;

(m) supervising and enforcing measures on essential and important entities in accordance with articles 29 and 30;

(n) ensuring effective, efficient and secure cooperation in the Cooperation Group and in the CSIRTs network:

Provided that in accordance with Article 47(1) of Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011, the Malta Financial Services Authority may participate in the activities of the Cooperation Group for matters that concern its supervisory activities in relation to financial entities:

Provided further that the Malta Financial Services Authority may request the CIP Department, to participate in the activities of the Cooperation Group for matters pertaining to essential or important entities, subject to such entities having been designated in accordance with this order as critical ICT third-party service providers in accordance with Article 31 of the said Regulation:

Provided further that the CIP Department shall exercise a *liaison* function as a single point of contact in accordance with this order, to ensure cross-border cooperation of Maltese authorities with the relevant authorities of other Member States and, where appropriate, with the European Commission and ENISA, as well as to ensure cross-sectoral cooperation with other competent authorities within Malta.

(3) Essential and important entities providing services in Malta as well as entities providing domain name registration services in Malta shall register on the national self-registration mechanism established by the CIP Department in accordance with sub-article 2(h), and shall provide at least the following information:

(a) the name of the entity;

(b) the name of the CSIRT providing monitoring services to the entity and whether it is an internal or autonomous CSIRT;

(c) the address and up-to-date contact details,

including email addresses, IP ranges and telephone numbers;

(d) where applicable, the relevant sector and sub-sector listed in the First or Second Schedule; and

(e) where applicable, a list of the Member States where they provide services falling within the scope of this order.

(4) The essential or important entities shall notify any changes to the details submitted in accordance with sub-article (3) without delay and, in any event, within two (2) weeks of the date of the change.

(5) The CIP Department shall also perform such related and consequential duties as the Minister may delegate from time to time.

(6) The Director shall represent the CIP Department in any judicial proceedings.

CSIRT.

8. (1) There shall be established a national CSIRT within the CIP Department, which shall comply with the requirements established in sub-article 9(1). It shall be responsible for incident handling in accordance with a well-defined process and shall cover at least the sectors, sub-sectors and types of entities listed in the First and Second Schedule.

(2) CSIRT shall:

(a) cooperate and, where appropriate, exchange relevant information in accordance with article 26 with sectoral or cross-sectoral communities of essential and important entities;

(b) participate in peer reviews organised in accordance with article 17; and

(c) act as the national representative to the CSIRT network.

(3) CSIRT may establish cooperation relationships with third countries' national CSIRTs subject to a cooperation agreement. The cooperation agreement shall facilitate effective, efficient and secure information exchange with those third countries' national CSIRTs, using relevant information-sharing protocols, including the Traffic Light Protocol.

(4) As part of such cooperation relationships, CSIRT may:

(a) exchange relevant information with third

countries' national CSIRTs, including personal data in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);

(b) cooperate with third countries' national CSIRTs or equivalent third-country bodies, in particular for the purpose of providing them with cybersecurity assistance.

Requirements of CSIRTs.

9. (1) All CSIRTs shall comply with the following requirements:

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

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

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

(d) the CSIRTs shall ensure the confidentiality and trustworthiness of their operations;

(e) the CSIRTs shall be adequately staffed to ensure availability of their services at all times, and they shall ensure that their staff is trained appropriately; and

(f) the CSIRTs shall be equipped with redundant systems and backup working space to ensure continuity of their services.

(2) The CSIRTs may participate in international cooperation networks.

Tasks of CSIRT and internal and autonomous CSIRTs.

10. (1) CSIRT shall have the following tasks:

(a) monitoring and analysing cyber threats, vulnerabilities and incidents at national level and, upon request, providing assistance to essential and important entities concerned regarding real-time or near real-time monitoring of their network and information systems;

(b) providing early warnings, alerts, announcements and dissemination of information to essential and important entities concerned as well as to the competent authorities and other relevant stakeholders on cyber threats, vulnerabilities and incidents, if possible in near real-time;

(c) responding to incidents and providing assistance to the essential and important entities concerned, where applicable;

(d) collecting and analysing forensic data and providing dynamic risk and incident analysis and situational awareness regarding cybersecurity;

(e) providing, upon the request of an essential or important entity, a proactive scanning of the network and information systems of the entity concerned to detect vulnerabilities with a potential significant impact;

(f) participating in the CSIRTs network and providing mutual assistance in accordance with their capacities and competencies to other members of the CSIRTs network upon their request;

(g) where applicable, acting as a coordinator for the purposes of the coordinated vulnerability disclosure in accordance with 13(1);

(h) contributing to the deployment of secure information-sharing tools.

(2) Internal and autonomous CSIRTs shall have at least the following tasks:

(a) monitoring and analysing cyber threats, vulnerabilities and incidents of the essential and important entities and providing real-time or near real-time monitoring of their network and information systems;

(b) providing early warnings, alerts, announcements and dissemination of information on cyber threats, vulnerabilities and incidents, if possible in near real-time to the essential and important entities;

(c) responding to incidents and providing assistance to the essential and important entities;

(d) collecting and analysing forensic data and providing dynamic risk and incident analysis and situational awareness regarding cybersecurity of the essential and

important entities;

(e) providing, a proactive scanning of the network and information systems of the essential and important entities to detect vulnerabilities with a potential significant impact:

Provided that the tasks referred to in this sub-article shall be carried out by internal and autonomous CSIRTs providing CSIRT monitoring services to essential and important entities in accordance with article 19(1)(d).

(3) CSIRT may carry out proactive non-intrusive scanning of publicly accessible network and information systems of essential and important entities. Such scanning shall be carried out to detect vulnerable or insecurely configured network and information systems and inform the entities concerned. Such scanning shall not have any negative impact on the functioning of the entities' services:

Provided that the essential and important entities shall be notified in writing of the proactive and non-intrusive scanning of their publicly accessible network and information systems, and following such scanning, shall be notified in writing of any vulnerable or insecurely configured network and information systems:

Provided further that CSIRT shall be deemed as duly authorised in the carrying out of this measure in accordance with article 337C(2) of the Criminal Code.

Cap. 9.

(4) When carrying out the tasks referred to in sub-article (1), CSIRT may prioritise particular tasks on the basis of a risk-based approach.

(5) CSIRT shall establish cooperation relationships with relevant stakeholders in the private sector, with a view to achieving the objectives of this order.

(6) In order to facilitate cooperation referred to in sub-article (5), CSIRT shall promote the adoption and use of common or standardised practices, classification schemes and taxonomies in relation to:

(a) incident-handling procedures;

(b) crisis management; and

(c) coordinated vulnerability disclosure in accordance with article 13(1).

Resources.

11. Adequate human, financial and technical resources shall be provided to the CIP Department, and CSIRT to carry out, in an

effective and efficient manner, the tasks assigned to them and thereby to fulfil the objectives of this order, in particular:

(a) to have the technical capabilities necessary to carry out the tasks referred to in article 10(1);

(b) to be allocated sufficient resources including adequate staffing levels and appropriate training for the purpose of enabling it to develop its technical capabilities; and

(c) to have at their disposal an appropriate, secure, and resilient communication and information infrastructure through which it shall exchange information with other essential and important entities and other relevant stakeholders.

Cooperation at national level.

12. (1) The CIP Department, CSIRT or where designated the competent authorities shall cooperate with each other with regard to the fulfilment of the obligations laid down in this order.

(2) CSIRT shall receive notifications of significant incidents in accordance with article 20 and incidents, cyber threats and near misses in accordance with article 27.

(3) CSIRT shall inform in writing the CIP Department and relevant competent authorities of notifications of incidents, cyber threats and near misses submitted in accordance with article 20(1).

(4) The CIP Department, and where designated the competent authority, and CSIRT shall cooperate with the Executive Police, the Information and Data Protection Commissioner in accordance with the Data Protection Act, the Head Aviation Security in accordance with the Airports and Civil Aviation (Security Act), the Civil Aviation Directorate in accordance with the Air Navigation Act, the Malta Communications Authority in accordance with the Electronic Commerce Act, Electronic Communications (Regulation) Act and the Radio Equipment Regulations, the Malta Financial Services Authority in accordance with Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) No 2016/1011, the CIP Department in accordance with Directive (EU) 2022/2557 as well as the competent authorities under other sector-specific Union legal acts, within Malta.

Cap. 586.
Cap. 405.
Cap. 641.
Cap. 426.
Cap. 399.
S.L. 427.41.

(5) The CIP Department and CSIRT shall exchange relevant information on a regular basis, including with regard to relevant incidents and cyber threats with competent authorities under this order, in particular with:

Cap. 399.
Cap. 426.

(a) the Malta Communications Authority in accordance with the Electronic Communications (Regulation) Act and the Electronic Commerce Act; and

(b) the Malta Financial Services Authority in accordance with Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

(6) The CIP Department, or where designated the competent authority under this order and the competent authority in accordance with Directive (EU) 2022/2557 shall cooperate and exchange information on a regular basis with regard to the identification of critical entities, on risks, cyber threats, and incidents as well as on non-cyber risks, threats and incidents affecting entities identified as critical entities under the said order, and the measures taken in response to such risks, threats and incidents.

(7) The reporting shall be simplified through technical means for notifications in articles 20 and 27.

(8) For the purposes of this regulation "competent authorities" means the Malta Communications Authority and the Malta Financial Services Authority.

Coordinated vulnerability disclosure.

13. (1) CSIRT shall be designated as coordinator for the purposes of coordinated vulnerability disclosure under this order.

(2) CSIRT shall act as a trusted intermediary and facilitating, where necessary, the interaction between the reporting natural or legal person and the entity making use of the potentially vulnerable ICT products, ICT processes or ICT services, upon the request of either party.

(3) The tasks of CSIRT designated as coordinator shall include:

(a) identifying and contacting the entities concerned;

(b) providing assistance to the natural or legal persons reporting a vulnerability;

(c) negotiating disclosure timelines and managing vulnerabilities that affect multiple entities; and

(d) establishing and maintaining a register of coordinated vulnerability disclosure policies.

(4) Persons shall be able to report, anonymously, a vulnerability to CSIRT. CSIRT shall ensure the anonymity and confidentiality of the persons throughout the vulnerability disclosure.

(5) CSIRT shall ensure that diligent follow-up action is carried out with regard to the reported vulnerability.

(6) Where a reported vulnerability may have a significant impact on entities in more than one Member State, CSIRT shall, where appropriate, cooperate with other CSIRTs designated as coordinators within the CSIRTs network.

(7) For the purposes of coordinated vulnerability disclosure, the reporting natural or legal person shall be deemed to have acted with authorisation in terms of article 337C of the Criminal Code, Cap. 9. insofar as the reporting natural or legal person complies with the coordinated vulnerability disclosure policy of such entity.

(8) CSIRT shall carry out the technical operations strictly necessary for the characterisation of the risk or threat referred to in this article.

Qualified auditors.

14. (1) An essential or important entity shall appoint a qualified auditor who shall verify if the entity has implemented the cybersecurity risk-management measures in accordance with article 19:

Provided that the qualified auditor shall satisfy the requirements listed in sub-article (4) before being appointed:

Provided further that if the qualified auditor satisfies the requirements listed in sub-article (4), the appointment shall be approved by the CIP Department, or where designated the competent authority.

(2) If the qualified auditor is unable to verify whether the essential or important entity has implemented the cybersecurity risk-management measures in accordance with article 19 he shall notify this in writing to the essential or important entity and the CIP Department, or where designated the competent authority.

(3) The CIP Department, or where designated the competent authority, shall ensure that the essential or important entity takes, without undue delay, all necessary, appropriate and proportionate corrective measures.

(4) The CIP Department, or where designated the competent authority, shall approve an appointment in accordance with sub-article (1), if the qualified auditor submits a reasoned request with accompanying documentation to the CIP Department, or where

designated the competent authority, demonstrating that he is:

(a) in possession of documentation attesting to a background check on the said auditor, issued by the competent authority in accordance with Directive (EU) 2022/2557;

(b) in possession of a valid European and, or international cybersecurity certification or cybersecurity standard; or

(c) experience and skillset as determined by the CIP Department:

Provided that in the case of essential entities, the qualified auditor shall satisfy all of the above requirements.

(5) The CIP Department shall maintain a list of qualified auditors and make this list available to essential and important entities.

(6) The CIP Department shall establish the procedure for the approval of the qualified auditor in accordance with sub-article (1).

PART III – NATIONAL CYBERSECURITY STRATEGY

National cybersecurity strategy.

15. (1) The National Cyber Security Steering Committee shall oversee the national cybersecurity strategy which established the strategic objectives, the resources required to achieve those objectives, and policy and regulatory measures with a view to achieving and maintaining a high level of cybersecurity in Malta.

(2) The national cybersecurity strategy shall include:

(a) objectives and priorities of the strategy on the security of network and information systems covering in particular the sectors, sub-sectors and types of entities listed in the First and Second Schedule;

(b) a governance framework to achieve the objectives and priorities referred to in sub-article (2)(a), including the policies referred to in sub-article (3);

(c) a governance framework defining the roles and responsibilities of relevant stakeholders at the national level, underpinning the cooperation and coordination at the national level between the competent authorities, the single point of contact, and the CSIRTs in accordance with this order, as well as coordination and cooperation between those bodies and competent authorities in accordance with sector-specific Union legal acts;

(d) a mechanism to identify relevant assets and an assessment of the risks in Malta;

(e) identification of the measures ensuring preparedness for, responsiveness to, and recovery from incidents, including cooperation between the public and private sectors;

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

(g) a policy framework for enhanced coordination between the competent authorities under this order and the competent authorities in accordance with in accordance with Directive (EU) 2022/2557 for the purpose of information sharing on risks, cyber threats, and incidents, as well as on non-cyber risks, threats and incidents and the exercise of supervisory tasks, as appropriate; and

(h) a plan, including necessary measures, to enhance the general level of cybersecurity awareness among citizens.

(3) The national cybersecurity strategy shall include the following policies:

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

(b) on the inclusion and specification of cybersecurity-related requirements for ICT products and ICT services in public procurement, including in relation to cybersecurity certification, encryption and the use of open-source cybersecurity products;

(c) managing vulnerabilities, encompassing the promotion and facilitation of coordinated vulnerability disclosure in accordance with article 13(1);

(d) related to sustaining the general availability, integrity and confidentiality of the public core of the open internet, including, where relevant, the cybersecurity of undersea communications cables;

(e) promoting the development and integration of relevant advanced technologies aiming to implement state-of-the-art cybersecurity risk-management measures;

(f) promoting and developing education and training

on cybersecurity, cybersecurity skills, awareness raising and research and development initiatives, as well as guidance on good cyber hygiene practices and controls, aimed at citizens, stakeholders and entities;

(g) supporting academic and research institutions to develop, enhance and promote the deployment of cybersecurity tools and secure network infrastructure;

(h) including relevant procedures and appropriate information-sharing tools to support voluntary cybersecurity information sharing between entities in conformity with Union law;

(i) strengthening the cyber resilience and the cyber hygiene baseline of small and medium-sized enterprises, in particular those excluded from the scope of this order, by providing easily accessible guidance and assistance for their specific needs; and

(j) promoting active cyber protection.

(4) The national cybersecurity strategy shall be assessed on a regular basis and at least every five (5) years on the basis of key performance indicators and, where necessary, be updated.

National cyber crisis management framework.

16. (1) There shall be established a national cyber crisis management framework which shall establish the management and coordination of large-scale cybersecurity incidents and crises in Malta, including the:

(a) identifying of capabilities, assets and procedures that may be deployed in the case of a large-scale cybersecurity incident or crisis for the purposes of this order; and

(b) drawing up of a national large-scale cybersecurity incident and crisis response plan where the objectives of, and arrangements for, the management of large-scale cybersecurity incidents and crises are established.

(2) The plan shall establish, in particular:

(a) the objectives of national preparedness measures and activities;

(b) the tasks and responsibilities of cyber crisis management authorities;

(c) the cyber crisis management procedures, including their integration into the general national crisis management

framework and information exchange channels;

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

(e) the relevant public and private stakeholders and infrastructure involved; and

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

(3) The crisis management authorities shall have adequate resources to carry out, in an effective and efficient manner, the tasks referred to in sub-article (2).

(4) The framework shall be coherent with the existing frameworks for general national crisis management.

(5) The CIP Department shall be the national representative for the purposes of cyber crisis management to the European cyber crisis *liaison* organisation network (EU CyCLONe) established in accordance with Article 16 of the Directive.

Peer reviews.

17. Prior to a commencement of a peer review on Malta, a self-assessment of the reviewed aspects may be carried out by the CIP Department in cooperation with CSIRT, designated competent entities and other entities and stakeholders where necessary and as appropriate. The CIP Department shall provide such self-assessment to the designated cybersecurity experts in accordance with Article 19 of the Directive.

PART IV – CYBERSECURITY RISK-MANAGEMENT MEASURES AND REPORTING OBLIGATIONS

Governance.

18. (1) The CIP Department, or where designated the competent authority, shall ensure that management bodies of such essential and important entities approve the cybersecurity risk-management measures in accordance with article 19 and oversee their implementation. The natural persons composing the management bodies may be held liable for infringements by the aforesaid entities of the said article in accordance with articles 31(10)(b) and 33.

(2) The application of sub-article (1) and this sub-article shall be without prejudice to national law as regards the liability rules applicable to public institutions, as well as the liability of public servants and elected or appointed officials.

(3) Members of the management bodies of essential and important entities are required to follow training in order to carry out their tasks.

(4) Essential and important entities shall offer similar training to their employees on a regular basis, in order that they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity.

Cybersecurity risk-management measures.

19. (1) The CIP Department, or where designated the competent authority, shall ensure that essential and important entities:

(a) take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services;

(b) ensure a level of security of network and information systems appropriate to the risks posed, taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in paragraph (a):

Provided that when assessing the proportionality of the measures, they shall take due consideration of the degree of the entity's exposure to risks, the entity's size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact;

(c) appoint a security *liaison* officer who shall have the necessary expertise and who shall:

(i) facilitate the development, implementation, maintenance and review of business continuity plans and where necessary termination plans that include the preparedness, processes and solutions of the essential or important entity;

(ii) ensure that the essential or important entity conducts and maintains appropriate risk assessments;

(iii) ensure that the essential or important entity maintains and exercises an operator security plan; and

(iv) act as the point of contact between the essential or important entity and the CIP Department, or

where designated the competent authority, to ensure the fulfilment of the obligations established in this order;

(d) receive CSIRT monitoring services from any of the following CSIRTs, which CSIRTs shall comply with the requirements established in article 9(1) and carry out the tasks set out in article 10(2):

(i) an internal CSIRT; or

(ii) an autonomous CSIRT.

(2) The measures in sub-article (1) shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

(a) policies on risk analysis and information system security;

(b) incident handling;

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

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

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

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

(g) basic cyber hygiene practices and cybersecurity training;

(h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;

(i) human resources security, insider risk management policy, access control policies and asset management;

(j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate; and

(k) logging and traceability of network and information systems.

(3) The CIP Department, or where designated the competent authority, shall ensure that, when considering which measures referred to in sub-article (2)(d) are appropriate, entities shall take into account the vulnerabilities specific to each direct supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures. The CIP Department, or where designated the competent authority, shall also ensure that, when considering which measures in the said sub-article are appropriate, entities are required to take into account the results of the coordinated security risk assessments of critical supply chains carried out in accordance with Article 22(1) of the Directive.

(4) The CIP Department, or where designated the competent authority, shall ensure that, where an essential or important entity finds that it does not comply with the measures provided for in sub-article (2), the entity concerned shall take, without undue delay, all necessary, appropriate and proportionate corrective measures referred to in article 29 for essential entities or article 30 for important entities.

Reporting obligations.

20. (1) Essential and important entities shall immediately notify CSIRT of any incident that has a significant impact on the provision of their services in accordance with sub-article (6):

Provided that the mere act of notification shall not subject the notifying entity to an increased liability:

Provided further that CSIRT shall immediately notify in writing any designated competent authority or authorities as the case may be, of any incident that has a significant impact on the provision of the services provided by an essential or important entity which such authority regulates.

(2) Where appropriate, essential and important entities shall notify, without undue delay, the recipients of their services of significant incidents that are likely to adversely affect the provision of those services. Those entities shall report any information enabling CSIRT to determine any cross-border impact of the incident.

(3) In the case of a cross-border or cross-sectoral significant incident, the CIP Department, shall be provided in due time with relevant information notified in accordance with sub-article (5).

(4) Where applicable, essential and important entities shall communicate, without undue delay, to the recipients of their services that are potentially affected by a significant cyber threat any measures

or remedies that those recipients are able to take in response to such threat. Where appropriate, the entities shall also inform those recipients of the significant cyber threat itself.

(5) For the purpose of notification in accordance with sub-article (1), the entities concerned shall submit to CSIRT:

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

(b) without undue delay and in any event within seventy-two (72) hours of becoming aware of the significant incident, an incident notification, which where applicable, shall update the information referred to in paragraph (a) and indicate an initial assessment of the significant incident, including its severity and impact, as well as where available, the indicators of compromise;

(c) upon the request of CSIRT an intermediate report on relevant status updates;

(d) a final report not later than one (1) month after the submission of the incident notification in accordance with sub-article (5)(b), including the following:

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

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

(iii) applied and ongoing mitigation measures;

(iv) where applicable, the cross-border impact of the incident;

(e) in the event of an ongoing incident at the time of the submission of the final report referred to in paragraph (d), the entities concerned shall provide CSIRT with a progress report at that time and a final report within one (1) month of their handling of the incident.

(6) By way of derogation from sub-article (5)(b), a trust service provider shall, with regard to significant incidents that have an impact on the provision of its trust services, notify CSIRT without undue delay and in any event within twenty-four (24) hours of

becoming aware of the significant incident.

(7) CSIRT shall provide, without undue delay and where possible within twenty-four (24) hours of receiving the early warning referred to in sub-article (5)(a), a response to the notifying entity, including initial feedback on the significant incident and, upon request of the entity, guidance or operational advice on the implementation of possible mitigation measures:

Provided that where CSIRT is not the initial recipient of the notification referred to in sub-article (1), the guidance shall be provided by the designated competent authority in cooperation with CSIRT. CSIRT shall provide additional technical support if the entity concerned so requests.

(8) Where the significant incident is reasonably suspected to be a criminal offence, CSIRT, or where designated the competent authority, shall also provide guidance on reporting the significant incident to the Executive Police.

(9) Where appropriate, and in particular where the significant incident concerns Malta and at least another Member State, CSIRT shall inform, without undue delay, the other affected Member State and ENISA of the significant incident and such information shall include the type of information received in accordance with sub-article (5):

Provided that in so doing, CSIRT shall, in accordance with national law and, or Union law, preserve the entity's security and commercial interests as well as the confidentiality of the information provided.

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

(11) At the request of CSIRT, or where designated the competent authority, the CIP Department shall forward notifications received in accordance with sub-article (1) to the single points of contact of other affected Member States.

(12) CSIRT shall provide to the CIP Department information about significant incidents, incidents, cyber threats and near misses notified in accordance with sub-article (1) and article 27.

(13) The CIP Department shall submit to ENISA, a summary

report, including anonymised and aggregated data on significant incidents, incidents, cyber threats and near misses notified in accordance with sub-article (1) and with article 27.

(14) Every three (3) months, the single point of contact shall submit to ENISA a summary report containing anonymised and aggregated data on significant incidents, incidents, cyber threats and near misses notified in accordance with sub-article (1) and article 27.

Use of European cybersecurity certification schemes.

21. (1) In the implementation of article 19 the CIP Department shall without imposing or discriminating in favour of any particular type of technology, encourage the use of ICT products, ICT services and ICT processes, developed by the essential or important entity or procured from third parties, that are certified under European cybersecurity certification schemes adopted in accordance with Article 49 of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act):

Provided that the CIP Department, or where designated the competent authority, shall require where applicable, essential and important entities to use such ICT products, ICT services and ICT processes:

Provided further that specific categories of essential and important entities listed in Commission delegated acts, shall use certain certified ICT products, ICT services and ICT processes or obtain a certificate under a European cybersecurity certification scheme adopted in accordance with Article 49 of Regulation (EU) 2019/881.

(2) Essential and important entities may use qualified trust services.

Standardisation.

22. In order to promote the convergent implementation of article 19(1) and (2), the CIP Department shall, without imposing or discriminating in favour of the use of a particular type of technology, encourage the use of European and international standards and technical specifications relevant to the security of network and information systems.

PART V – JURISDICTION AND REGISTRATION

Jurisdiction and territoriality.

23. (1) Entities falling within the scope of this order shall be considered to fall under the jurisdiction of Malta if they are established in Malta, except in the case of:

(a) providers of public electronic communications

networks or providers of publicly available electronic communications services, which shall be considered to fall under the jurisdiction of the Member State in which they provide their services;

(b) DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines or of social networking services platforms, which shall be considered to fall under the jurisdiction of the Member State in which they have their main establishment in the Union in accordance with sub-article (2);

(c) public administration entities, which shall be considered to fall under the jurisdiction of the Member State which established them.

(2) For the purposes of this order, an entity as provided for in in sub-article (1)(b), shall be considered to have its main establishment in the Union, in the Member State where the decisions related to the cybersecurity risk-management measures are predominantly taken:

Provided that, if such a Member State cannot be determined or if such decisions are not taken in the Union, the main establishment shall be considered to be in the Member State where cybersecurity operations are carried out.

Provided further that, if such a Member State cannot be determined, the main establishment shall be considered to be in the Member State where the entity concerned has the establishment with the highest number of employees in the Union.

(3) If an entity in sub-article (1)(b), is not established in the Union, but offers services within the Union, it shall designate a representative in the Union and such representative shall be established in one (1) of those Member States where the services are offered. Such an entity shall be considered to fall under the jurisdiction of the Member State where the representative is established.

(4) In the absence of a representative in the Union designated in accordance with sub-article (3), the CIP Department or, where designated, the competent authority, may take legal action against the entity for the infringement of this order where the entity provides services in Malta.

(5) The designation of a representative by an entity as

provided for in sub-article (1)(b), shall be without prejudice to legal action which could be initiated against the entity itself.

(6) Upon a request for mutual assistance in relation to an entity in sub-article (1)(b), the CIP Department or, where designated, the competent authority may, within the limits of such request, take appropriate supervisory and enforcement measures in relation to the entity concerned that provides services or which has a network and information system in Malta.

Registry of entities.

24. (1) DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines and of social networking services platforms shall submit to the CIP Department, by the prescribed date, the following information:

(a) the name of the entity;

(b) the relevant sector, sub-sector and type of entity in the First or Second Schedule, where applicable;

(c) the address of the entity's main establishment and its other legal establishments in the Union or, if not established in the Union, of its representative designated pursuant to article 23(3);

(d) up-to-date contact details, including email addresses and telephone numbers of the entity and, where applicable, its representative designated pursuant to article 23(3);

(e) the Member States where the entity provides services;

(f) the entity's IP ranges; and

(g) a detailed list of computer, network and operational technology resources used.

(2) The entities in sub-article (1) shall notify the CIP Department about any changes to the information they submitted without delay and in any event within three (3) months of the date of the change:

Provided that the entity shall provide information in accordance with sub-article (1)(g) to the CIP Department upon request.

(3) Upon receipt of the information provided for in sub-articles (1) and (2), except for that provided for in sub-articles (1)(f) and (g), the CIP Department shall, without undue delay, forward such information to ENISA.

(4) Where applicable, the information provided for in sub-articles (1) and (2) shall be submitted through the national self-registration mechanism provided for in sub-article 7(3).

(5) By 17 April 2025 and every two (2) years thereafter, the CIP Department shall notify:

(a) the European Commission and the Cooperation Group of the number of essential and important entities listed pursuant to article 7(2)(i) for each sector and sub-sector in the First or Second Schedule; and

(b) the European Commission of relevant information about the number of essential and important entities identified pursuant to sub-articles (1)(b) to (e), the sector and sub-sector provided for in the First or Second Schedule to which they belong, the type of service that they provide, and the provision, from among those established in sub-articles (1)(b) to (e), pursuant to which they were identified.

(6) Until 17 April 2025 and upon request of the European Commission, Malta may notify the European Commission of the names of the essential and important entities provided for in sub-article (5)(b).

Database of domain name registration data.

25. (1) For the purpose of contributing to the security, stability and resilience of the DNS, the CIP Department shall require TLD name registries and entities providing domain name registration services to collect and maintain accurate and complete domain name registration data in a dedicated database with due diligence in accordance with European Union law in relation to information which constitutes personal data.

(2) For the purposes of sub-article (1), the database of domain name registration data shall contain the necessary information to identify and contact the holders of the domain names and the points of contact administering the domain names under the TLDs. Such information shall include:

(a) the domain name;

(b) the date of registration;

(c) the registrant's name, contact email address and telephone number;

(d) the contact email address and telephone number of the point of contact administering the domain name in the event that they are different from those of the registrant.

(3) The TLD name registries and the entities providing domain name registration services shall have in place policies and procedures, including verification procedures, to ensure that the databases in sub-article (1) include accurate and complete information. Such policies and procedures shall be made publicly available.

(4) The TLD name registries and the entities providing domain name registration services shall make publicly available, without undue delay after the registration of a domain name, the domain name registration data which are not personal data.

(5) The TLD name registries and the entities providing domain name registration services shall provide access to specific domain name registration data upon lawful and duly substantiated requests by legitimate access seekers, in accordance with national data protection legislation and Union data protection law. The TLD name registries and the entities providing domain name registration services shall reply without undue delay and in any event within seventy-two (72) hours of receipt of any requests for access. Policies and procedures with regard to the disclosure of such data shall be made publicly available:

Provided that domain name registration data shall be free of charge to legitimate access seekers upon lawful and duly substantiated requests.

(6) Compliance with the obligations established in sub-articles (1) to (5) shall not result in a duplication of collecting domain name registration data. To that end, TLD name registries and entities providing domain name registration services shall cooperate with each other.

PART VI – INFORMATION SHARING

Cybersecurity information-sharing arrangements.

26. (1) CSIRT shall ensure that the entities falling within the scope of this order and, where relevant, other CSIRTs of entities not falling within the scope of this order are able to exchange on a voluntary basis relevant cybersecurity information among themselves, including information relating to cyber threats, near misses, vulnerabilities, techniques and procedures, indicators of compromise, adversarial tactics, threat-actor-specific information, cybersecurity alerts and recommendations regarding the configuration of cybersecurity tools to detect cyberattacks, where such information sharing:

(a) aims to prevent, detect, respond to or recover from incidents or to mitigate their impact;

(b) enhances the level of cybersecurity, in particular through raising awareness in relation to cyber threats, limiting or impeding the ability of such threats to spread, supporting a range of defensive capabilities, vulnerability remediation and disclosure, threat detection, containment and prevention techniques, mitigation strategies, or response and recovery stages or promoting collaborative cyber threat research between public and private entities:

Provided that the cybersecurity information sharing arrangement shall be without prejudice, to the operator security plan of the entities falling within the scope of this order, pursuant to article 19(1)(c)(iii).

(2) CSIRT shall ensure that the exchange of information takes place within communities of essential and important entities, and where relevant, their suppliers or service providers. Such exchange shall be implemented by means of cybersecurity information-sharing arrangements in respect of the potentially sensitive nature of the information shared.

(3) CSIRT, shall facilitate the establishment of cybersecurity information-sharing arrangements in sub-article (2). Such arrangements may specify operational elements, including the use of dedicated ICT platforms and automation tools, content and conditions of the information-sharing arrangements:

Provided that, in establishing the details of the involvement of public authorities in such arrangements, CSIRT may impose conditions on the information made available by any competent authority or CSIRT. CSIRT shall offer assistance for the application of such arrangements in accordance with its policies provided for in article 15(3)(h).

(4) Essential and important entities shall notify the CIP Department of their participation in the cybersecurity information-sharing arrangements provided for in sub-article (2), upon entering into such arrangements, or as applicable, of their withdrawal from such arrangements, once the withdrawal takes effect.

Voluntary notification of relevant information.

27. (1) In addition to the notification obligation provided for in article 20, notifications may be submitted to CSIRT on a voluntary basis by:

(a) essential and important entities with regard to incidents, cyber threats and near misses;

(b) entities other than those in sub-article (1)(a), regardless of whether they fall within the scope of this order, with regard to significant incidents, cyber threats and near misses.

(2) CSIRT shall process the notifications in sub-article (1) in accordance with the procedure established in article 20 and may prioritise the processing of mandatory notifications over voluntary notifications.

(3) Where applicable, CSIRT shall provide the CIP Department and where designated the competent authority, with the information about notifications received pursuant to this article, while ensuring the confidentiality and appropriate protection of the information provided by the notifying entity.

(4) Without prejudice to the prevention, investigation, detection and prosecution of criminal offences, voluntary reporting shall not result in the imposition of any additional obligations upon the notifying entity to which it would not have been subject had it not submitted the notification.

PART VII – SUPERVISION AND ENFORCEMENT

General aspects concerning supervision and enforcement.

28. (1) The CIP Department, or where designated the competent authority, shall effectively supervise and take the measures necessary to ensure compliance with this order.

(2) The CIP Department, or where designated the competent authority, may prioritise on a risk-based approach the supervisory tasks provided for in articles 29 and 30:

Provided that when exercising such prioritisation, the CIP Department, or where designated the competent authority, shall establish supervisory methodologies allowing for a prioritisation of such tasks following a risk-based approach.

(3) The CIP Department, or where designated the competent authority, shall work in close cooperation with the Information and Data Protection Commissioner when addressing incidents resulting in personal data breaches, and this is without prejudice to the competence and tasks of the Information and Data Protection Commissioner under Regulation (EU) 2016/679.

(4) Without prejudice to national legislative and institutional frameworks in the supervision of compliance of public administration entities with this order and the imposition of enforcement measures with regard to infringements of this order the CIP Department, or where designated the competent authority, shall carry out such tasks

with operational independence from the public administration entities being supervised:

Provided that the enforcement measures in article 31(10)(a) and (b) shall not be applicable to public administration entities subject to this order.

Supervisory and enforcement measures in relation to essential entities.

29. (1) The CIP Department, or where designated the competent authority, shall ensure that the supervisory or enforcement measures imposed on essential entities in respect of the obligations established in this order are effective, proportionate and dissuasive, taking into account the circumstances of each individual case:

Provided that the implementation of such supervisory and, or enforcement measures shall be without prejudice to article 3(16).

(2) When exercising the supervisory tasks in relation to essential entities, the CIP Department, or where designated the competent authority, shall have the power to subject those entities at least to the following supervisory measures:

(a) on-site inspections and off-site supervision, including random checks conducted by trained professionals;

(b) regular and targeted security audits carried out by an independent body, or the CIP Department, or where designated the competent authority;

(c) *ad hoc* audits, including where justified on the ground of a significant incident or an infringement of this order by the essential entity concerned;

(d) security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria, where necessary with the cooperation of the essential entity concerned;

(e) requests for information necessary to assess the cybersecurity risk-management measures adopted by the essential entity concerned, including documented cybersecurity policies, as well as compliance with the obligation to submit information to the CIP Department, pursuant to article 24;

(f) requests to access data, documents and information necessary for the CIP Department, or where designated the competent authority, to carry out 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;

(h) requests for evidence of CSIRT monitoring services in accordance with article 19(1)(d);

(i) requests for evidence of compliance with policies issued by the CIP Department, or where designated the competent authority, by the CSIRT providing monitoring services to the essential entity;

(j) requests for evidence of operator security plans, business continuity plans and where necessary termination plans;

(k) any other supervisory measures which the CIP Department, or where designated the competent authority shall consider necessary in accordance with its powers at law.

(3) The targeted security audits in sub-article (2)(b), shall be based on risk assessments conducted by the CIP Department, or where designated the competent authority or the audited essential entity, or on other risk-related available information.

(4) The results of any targeted security audit in sub-articles (2)(b) and (3), shall be made available to the CIP Department, or where designated the competent authority. The costs of such targeted security audit carried out by an independent body shall be paid by the audited essential entity, except in duly substantiated cases when the CIP Department, or where designated the competent authority shall decide otherwise:

Provided that the CIP Department shall establish the principles in relation to targeted security audits, which may qualify for an exception under this sub-article:

Provided further that any decision taken by the CIP Department, or where designated the competent authority, in relation to the costs may be appealed before the Tribunal.

(5) When exercising the supervisory powers under sub-articles (2)(e) to (j), the CIP Department, or where designated, the competent authority, shall state the purpose of the request and specify the information requested.

(6) When exercising enforcement powers in relation to an essential entity, the CIP Department, or where designated the competent authority, shall have the power to take any or all of the following enforcement measure:

(a) issue warnings about infringements of this order by the essential entity concerned including but not limited to failure to cooperate or comply with any of the supervisory measures under sub-article (2);

(b) adopt binding instructions, including with regard to measures necessary to prevent or remedy an incident, as well as time-limits for the implementation of such measures and for reporting on their implementation, or an order requiring the essential entity concerned to remedy the deficiencies identified or the infringements of this order;

(c) order the essential entity concerned to cease conduct that infringes this order and desist from repeating that conduct;

(d) order the essential entity concerned to ensure that their cybersecurity risk-management measures comply with article 19 and, or to fulfil the reporting obligations established in article 20, in a specified manner and within a specified period;

(e) order the essential entity concerned to inform the natural or juridical persons with regard to which they provide services or carry out activities which are potentially affected by a significant cyber threat, of the nature of the threat, as well as of any possible protective or remedial measures which can be taken by those natural or juridical persons in response to such threat;

(f) order the essential entity concerned 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 for a determined period of time to oversee the compliance of the essential entity concerned with articles 19 and 20;

(h) order the essential entity concerned to make public aspects of infringements of this order in a specified manner;

(i) order the essential entity concerned to receive CSIRT monitoring services in accordance with article 19(1)(d);

(j) order the essential entity concerned to register under the national self-registration mechanism in article 7(3);

(k) any other enforcement measure which the CIP Department, or where designated the competent authority, shall consider necessary in accordance with its powers at law.

(7) In addition to the enforcement measures in sub-articles (6)(a) to (k), the CIP Department, or where designated the competent authority, may request the imposition of an administrative penalty by the Civil Court, in accordance with national law pursuant to article 33.

(8) The CIP Department, or where designated the competent authority, may impose the measures contained in this article on essential entities periodically.

(9) The CIP Department, or where designated the competent authority, shall inform the competent authority established in accordance with Directive (EU) 2022/2557 when exercising supervisory and enforcement powers aiming to ensure compliance of an essential entity identified as a critical entity in accordance with the said Directive:

Provided that, where required, such essential entity may request the CIP Department, or where designated the competent authority, to exercise supervisory and enforcement powers in relation to an essential entity that is identified as a critical entity in accordance with Directive (EU) 2022/2557.

Supervisory and enforcement measures in relation to important entities.

30. (1) When provided with evidence, indication or information that an important entity allegedly does not comply with this order, in particular articles 19 and, or 20, the CIP Department, or where designated the competent authority, shall take action, where necessary, through *ex post* supervisory measures. Such measures shall be effective, proportionate and dissuasive, taking into account the circumstances of each individual case:

Provided that the implementation of such supervisory tasks and, or enforcement measures shall be without prejudice to article 3(16).

(2) When exercising their supervisory tasks in relation to important entities, the CIP Department, or where designated the competent authority, shall have the power to subject such entities at least to the following supervisory measures:

(a) on-site inspections and off-site *ex post* supervision conducted by trained professionals;

(b) targeted security audits carried out by an independent body or the CIP Department, or where designated the competent authority;

(c) security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria, where necessary with the cooperation of the essential entity

concerned;

(d) requests for information necessary to assess, *ex post*, the cybersecurity risk-management measures adopted by the essential entity concerned, including documented cybersecurity policies, as well as compliance with the obligation to submit information to the CIP Department, or where designated the competent authority, pursuant to article 24;

(e) requests to access data, documents and information necessary to carry out their supervisory tasks;

(f) 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;

(g) requests for evidence of CSIRT monitoring services in accordance with article 19(1)(d);

(h) requests for evidence of compliance with policies issued by the CIP Department, or where designated the competent authority, by the CSIRT providing monitoring services to the important entity;

(i) requests for evidence of operator security plans, business continuity plans and where necessary termination plans;

(j) any other supervisory measures which the CIP Department, or where designated the competent authority considers necessary in accordance with its powers at law.

(3) The targeted security audits provided for in sub-article (2)(b), shall be based on risk assessments conducted by the CIP Department or the audited entity, or on other risk-related available information.

(4) The results of any targeted security audit shall be made available to the CIP Department, or where designated the competent authority. The costs of such targeted security audit carried out by an independent body shall be paid by the audited entity, except in duly substantiated cases when the CIP Department or, where designated the competent authority decide otherwise:

Provided that the CIP Department shall establish the principles in relation to targeted security audits, which may qualify for an exception under this sub-article:

Provided further that any decision taken by the CIP

Department, or where designated the competent authority, in relation to the allocation of costs may be appealed before the Tribunal.

(5) When exercising its powers in accordance with sub-articles (2)(d) to (f), the CIP Department, or where designated the competent authority, shall state the purpose of the request and specify the information requested.

(6) When exercising enforcement powers in relation to important entities, the CIP Department, or where designated the competent authority, shall have the power to take any or all of the following measures:

(a) issue warnings about infringements of this order by the important entity concerned including the failure to cooperate or comply with the supervisory measures under sub-article (2);

(b) adopt binding instructions, including with regard to measures necessary to prevent or remedy an incident, as well as time-limits for the implementation of such measures and for the reporting of the implementation, or an order requiring the essential entity concerned to remedy the deficiencies identified or the infringements of this order;

(c) order the important entity concerned to cease conduct that infringes this order and desist from repeating such conduct;

(d) order the important entity concerned to ensure that its cybersecurity risk-management measures comply with article 19 and, or to fulfil the reporting obligations established in article 20, in a specified manner and within a specified period;

(e) order the important entity concerned to inform the natural or juridical persons with regard to which they provide services or carry out activities which are potentially affected by a significant cyber threat, of the nature of the threat, as well as of any possible protective or remedial measures which can be taken by those persons in response to such threat;

(f) order the important entity concerned to implement the recommendations provided as a result of a security audit within a reasonable deadline;

(g) order the important entity concerned to make public aspects of infringements of this order in a specified manner;

(h) order the important entity concerned to receive CSIRT monitoring services in accordance with article 19(1)(d);

(i) order the important entity concerned to register itself under the national self-registration mechanism in accordance with article 7(3); and, or

(j) any other enforcement measures which the CIP Department, or where designated the competent authority considers necessary in accordance with their powers at law.

(7) In addition to the enforcement measures in sub-article (6)(a) to (j), the CIP Department or where designated the competent authority, may request the imposition of an administrative penalty by the Civil Court in accordance with national law pursuant to article 34.

Proceedings for the imposition of enforcement measures.

31. (1) The CIP Department, or where designated the competent authority, shall before proceeding to imposing the enforcement measures in accordance with articles 29 and 30, notify in writing the preliminary findings of an infringement to the essential or important entity concerned, of the measure that may be taken and the detailed reason why it may be taken by the CIP Department, or where designated the competent authority, requiring the essential or important entity concerned to make its submissions to the CIP Department, or where designated the competent authority, in a period not exceeding fifteen (15) working days and to propose any remedies that rectify the acts or omissions required by the CIP Department, or where designated the competent authority, to be so rectified:

Provided that the request for the imposition of an administrative penalty in accordance with articles 29(7) and 30(7) shall not be considered an enforcement measure.

(2) The period in sub-article (1), may be decreased if the CIP Department, or where designated the competent authority, considers that the continuance of an infringement under this order negatively impacts the effective exercise by the CIP Department, or where designated the competent authority, of its regulatory functions or warrants the immediate intervention of the CIP Department, or where designated the competent authority.

(3) Without prejudice to sub-article (2), where the CIP Department, or where designated the competent authority, has *prima facie* evidence that an infringement represents an immediate and significant incident in Malta, they may take any urgent interim enforcement measure to remedy the situation in advance of issuing the final enforcement measure, including ordering the immediate cessation of the act or omission giving cause to the infringement:

Provided that urgent interim enforcement measures shall be valid for a maximum period of three (3) months.

(4) Where the essential or important entity concerned remedies the deficiency within the period established in sub-article (1) and, or (3), and agrees in writing to abide with any enforcement measure that the CIP Department, or where designated the competent authority, may impose, the CIP Department, or where designated the competent authority, may desist from proceeding any further, without prejudice to any urgent interim enforcement measure imposed pursuant to sub-article (3) and, or enforcement measure that may have already been imposed.

(5) If after the lapse of the period established in sub-article (1) and, or (3), the CIP Department, or where designated the competent authority, considers that the essential or important entity concerned has not given any valid reason to demonstrate why no enforcement measure or measures should be taken against the entity, the CIP Department, or where designated the competent authority, shall notify in writing the essential or important entity concerned, stating the enforcement measure or measures intended to be taken.

(6) The notice in sub-article (5) shall, upon the expiry of the periods in sub-articles (1) and, or (3), and upon the service of a copy of the notice thereof, by means of a judicial act on the essential or important entity concerned indicated in the notice, constitute an executive title for all effects and purposes of Title VII of Book Second of the Code of Organization and Civil Procedure: Cap. 12.

Provided that if the essential or important entity concerned against which the notice has been issued, files an appeal within the twenty (20) working day period in accordance with article 42(2), and concurrently with or before the filing of its appeal, requests the suspension of the effects of the notice, the CIP Department, or where designated the competent authority, shall desist from issuing a judicial act in accordance with this sub-article until such time as the request for suspension has been determined, withdrawn or otherwise dealt with:

Provided further that the Tribunal may determine any requests for suspension in this sub-article expeditiously and in any case in a period not exceeding seven (7) working days. Before determining any such request, the Tribunal shall give the CIP Department, or where designated the competent authority, an opportunity to reply and make its submissions, within a period of at least three (3) working days.

(7) The effect of an enforcement measure imposed by the CIP Department, or where designated the competent authority, to

which an appeal relates, shall not except where so ordered, be suspended in consequence of the bringing of the appeal.

(8) When taking any of the enforcement measures in articles 29 and 30, the CIP Department, or where designated the competent authority, shall take account of the circumstances of each individual case and, as a minimum, take due account of:

(a) the seriousness of the infringement, the importance of the provisions breached under this order, including the possible delay in ceasing or rectifying the acts or omissions bringing about the infringement, with the following, *inter alia*, constituting a serious infringement in any event:

(i) repeated violations;

(ii) a failure to notify or remedy significant incidents;

(iii) a failure to remedy deficiencies following binding instructions from the CIP Department, or where designated the competent authority;

(iv) the obstruction of audits or monitoring activities ordered by the CIP Department, or where designated the competent authority following the finding of an infringement;

(v) providing false or grossly inaccurate information in relation to cybersecurity risk-management measures or reporting obligations established in articles 19 and, or 20;

(b) the duration of the infringement;

(c) any relevant previous infringements by the essential entity;

(d) any material or non-material damage caused, including any financial or economic loss, effects on other services and the number of users affected;

(e) any intent or negligence on the part of the perpetrator of the infringement;

(f) any measure taken by the essential entity to prevent or mitigate the material or non-material damage;

(g) any adherence to approved codes of conduct or approved certification mechanisms; and

(h) the level of cooperation of the persons held responsible with the CIP Department.

(9) Where enforcement measures imposed by the CIP Department, or where designated the competent authority, pursuant to sub-article (6) are ineffective, the essential entity concerned shall have a period not being less than fifteen (15) working days in which to take the necessary action to remedy the deficiencies and, or to comply with the requirements imposed by the CIP Department, or where designated the competent authority.

(10) If the requested action is not taken within the stipulated period in sub-article (9), the CIP Department, or where designated the competent authority, shall have the power to:

(a) request the certification or authorisation body, courts or tribunals in conformity with national law to suspend temporarily a certification or authorisation concerning part or all of the relevant services provided or activities carried out by the essential entity, or all of them;

(b) request the Civil Court in conformity with national law to prohibit temporarily any natural person who is responsible for discharging managerial responsibilities of chief executive officer or legal representation in the essential entity from exercising managerial functions in such essential entity:

Provided that temporary suspensions or prohibitions imposed pursuant to this sub-article shall be applied only until the essential entity concerned takes the necessary action to remedy the deficiencies or comply with the requirements of the CIP Department, or where designated the competent authority for which such enforcement measures were applied:

Provided further that the imposition of such temporary suspensions or prohibitions shall be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter, including the right to an effective remedy and to a fair trial, the presumption of innocence and the rights of the defence.

General conditions for imposing administrative penalties on essential and important entities.

32. (1) The administrative penalties shall be imposed in addition to any of the enforcement measures in article 29(6)(a) to (k), article 30(6)(a) to (k) and article 31(10).

(2) Where the CIP Department, or where designated the competent authority, requests the imposition of an administrative penalty and in doing so, determines the amount of the administrative penalty in each individual case, due regard shall be given, to the elements provided for in article 31(8).

(3) When they infringe articles 19 or 20, essential entities are subject, in accordance with sub-articles (1) and (2), to administrative penalties of a maximum of ten million euro (€10 000 000), or of a maximum of two percent (2%) of the total worldwide annual turnover in the preceding financial year of the undertaking to which the essential entity belongs, whichever is higher.

(4) When they infringe articles 19 or 20, important entities are subject, in accordance with sub-articles (1) and (2), to administrative penalties of a maximum of seven million euro (€7 000 000), or of a maximum of one point four percent (1.4%) of the total worldwide annual turnover in the preceding financial year of the undertaking to which the essential entity belongs, whichever is higher.

(5) Without prejudice to the powers of the CIP Department, or where designated the competent authority, administrative penalties may be imposed against public administration entities.

(6) Interest at the rate of five percent (5%) or such other rates as may be established by the Minister for Finance from time to time shall run as from the date set by the CIP Department, or where designated the competent authority, for the payment of any administrative penalty imposed by the Civil Court in terms of this order by which the CIP Department, or where designated the competent authority are entitled to enforce. Where the Civil Court or the Court of Appeal, as the case may be, after having upheld an application to suspend the penalty pending proceedings, finally decides that the penalty is due, such penalty shall be due together with any interests accrued thereon as from the date originally set by the CIP Department, or where designated the competent authority for payment including the period during which the payment of the said penalty was suspended.

Recommen-dations by the Advisory Board on the imposition of administrative penalties.

33. (1) Whenever the Advisory Board finds that an essential or important entity infringes or fails to comply with any of the provisions referred to article 34(1)(a) to (c), it shall issue relevant recommendations to the CIP Department.

(2) The Advisory Board in its recommendations, shall provide the amount of the administrative penalty and a specified time within which the entity concerned is to pay the administrative penalty:

Provided that the Advisory Board may, if it deems necessary, ask for more information or documentation from the CIP Department.

Proceedings for the imposition of administrative penalties.

34. (1) Independently of whether a penalty is issued upon the entity concerned, the CIP Department, or where designated the competent authority may, in accordance with article 31 require the entity to comply with the following provisions as applicable:

(a) cybersecurity risk-management measures and, or reporting obligations in articles 19 and 20;

(b) enforcement measures in article 29(6)(a) to (k), article 30(6)(a) to (j) and article 31(10);

(c) any other law or measure applicable to ensure compliance and enforcement, taken by the CIP Department, or where designated the competent authority.

(2) The CIP Department, or where designated the competent authority, shall also notify the entity concerned of the following:

(a) the administrative penalty that may be imposed by the Civil Court following the institution of legal proceedings;

(b) the specific reason why the administrative penalty may be imposed;

(c) the amount of the administrative penalty;

(d) the timeframe within which the entity concerned shall pay the administrative penalty:

Provided that the timeframe referred to in article 34(2)(d) shall be not more than twenty (20) working days or not less than five (5) working days from the date of service of the notice:

Provided further that the CIP Department, or where designated the competent authority, shall seek the advice of the Advisory Board in accordance with article 33 before initiating the process for the imposition of an administrative penalty:

Provided further that the essential or important entity shall be given an opportunity during such period of time as may be stipulated in the notice to make submissions to the CIP Department, or where designated the competent authority.

(3) In the notice mentioned in sub-article (1), the CIP Department, or where designated the competent authority, may impose such conditions as it may consider reasonable in the circumstances.

(4) If the essential or important entity concerned against which the notice has been issued, files an appeal before the Civil Court and concurrently with or before the filing of its appeal, requests the suspension of the effects of the notice, the CIP Department, or where designated the competent authority, shall desist from issuing a judicial act in accordance with this sub-article until such time as the request for suspension has been determined, withdrawn or otherwise dealt with.

(5) Notwithstanding the provisions of any other law, no precautionary warrant or order shall be issued by any court restraining the CIP Department, or where designated the competent authority, from exercising any of the powers conferred upon it under this order in relation to administrative penalties.

(6) An administrative penalty imposed by the Civil Court upon the essential or important entity shall be considered a civil debt owing to the CIP Department, or where designated the competent authority.

Debt recovery and procedure. Cap. 12.

35. The provisions of article 466 of the Code of Organization and Civil Procedure shall *mutatis mutandis* apply to the administrative penalties established by this order.

Sworn application for the imposition of an administrative penalty.

36. (1) Where the CIP Department, or where designated the competent authority, institutes proceedings to request the imposition of an administrative penalty pursuant to sub-articles 29(7) or 30(7), it shall proceed by sworn application before the Civil Court.

(2) The sworn application referred to in sub-article (1) shall:

(a) state the facts which led the CIP Department, or where designated the competent authority, to request the imposition of an administrative penalty by the Civil Court;

(b) contain a request by the CIP Department, or where designated the competent authority, for the Civil Court to deliver a judgement against the essential or important entity concerned; and

(c) where applicable, contain a request by the CIP Department, or where designated the competent authority, for the imposition of a daily administrative penalty in accordance with article 38:

Provided that the CIP Department, or where designated the competent authority, may also indicate a specific amount of the administrative penalty in its sworn application or by a note presented in the Civil Court during proceedings:

Provided further that the provisions of article 156 of the Code of Organization and Civil Procedure shall, where applicable, also apply to the sworn application.

Cap. 12.

(3) The CIP Department, or where designated the competent authority, may also include a report in the Maltese or English language with the findings during the carrying out of the supervisory tasks.

(4) The essential or important entity concerned against whom the sworn application is served, shall file by not later than twenty (20) days from date of service, a sworn reply and in this case the provisions of article 158 of the Code of Organization and Civil Procedure shall *mutatis mutandis* apply.

Cap. 12.

(5) Judicial proceedings shall be subject to appropriate procedural safeguards in accordance with the general principles of national and Union law and the Charter, including the right to an effective remedy and to a fair trial, the presumption of innocence and the rights of the defence.

Representation of entity and liability for breach of duties.

37. (1) Any natural person having the legal and judicial representation of the essential or important entity concerned, including the authority to take decisions on its behalf or, the authority to exercise control of it, shall have the power to ensure its compliance with this order and shall be liable for breach of his duties in case of non-compliance of the essential or important entity by means of an infringement of this order in particular articles 19 and, or 20:

Provided that this sub-article shall be without prejudice to national law regulating the liability of public servants and elected or appointed officials.

(2) If the natural person is found in breach of his duties, in case of non-compliance of the essential or important entity with this order, the CIP Department, or where designated the competent authority, may proceed against such natural person under sub-article 31(10)(b).

Daily administrative penalty payments.

38. (1) The CIP Department, or where designated the competent authority, may request the imposition by the Civil Court of daily administrative penalty payments for each infringement which the essential or important entity concerned repeatedly fails to cease and, or rectify, in accordance with a prior decision of the CIP Department, or where designated the competent authority.

(2) The daily administrative penalty payment shall be one hundred euro (€100) for each infringement for each day during which each infringement in sub-article (1) persists, which administrative penalty payment shall be determined by the CIP Department, or where designated the competent authority:

Provided that any daily administrative penalty payment imposed, may be backdated to the date when the breach was committed or the infringement started.

Infringements entailing a personal data breach.

39. (1) Where the CIP Department, or where designated the competent authority, becomes aware in the course of supervision or enforcement that the infringement by an essential or important entity

of the obligations established in articles 19 and, or 20 may entail a personal data breach, as defined in Article 4(12) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) which is to be notified in accordance with Article 32 of the said Regulation, it shall without undue delay, inform the Information and Data Protection Commissioner.

(2) Where the Information and Data Protection Commissioner imposes an administrative penalty in accordance with Article 58(2)(i) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), the CIP Department, or where designated the competent authority, shall not request the imposition of an administrative penalty in accordance with article 34 for an infringement in sub-article (1) arising from the same conduct as that which was the subject of the administrative penalty under Article 58(2)(i) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). The CIP Department, or where designated the competent authority, may however, impose the enforcement measures provided for in sub-article 29(6)(a) to (k), sub-article 30(6)(a) to (k) and sub-article 31(10).

(3) Where the supervisory authority competent in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), is not established in Malta, the CIP Department, or where designated the competent authority, shall inform the Information and Data Protection Commissioner of the potential data breach referred to in sub-article (1).

Mutual assistance.

40. (1) Where an entity provides services in Malta and in other Member States, or provides services in Malta or in other Member States and its network and information systems are located in Malta and in other Member States, the CIP Department, or where designated the competent authority, shall cooperate with and assist competent authorities of the Member States concerned as necessary. Such cooperation shall entail, at least, that:

(a) when the CIP Department, or the designated competent authority, apply supervisory and, or enforcement measures in Malta, the CIP Department, or where designated the competent authority, shall inform and consult the competent authorities in the other Member States concerned on the supervisory and, or enforcement measures taken:

Provided that the designated competent authority shall notify in writing the Malta CIP Department, or where designated the competent authority, of the application of such supervisory and, or enforcement measures in Malta;

(b) the Malta CIP Department, or where designated the competent authority, may request the competent authority of another Member State to take supervisory and enforcement measures in Malta:

Provided that such measures are exercised under the guidance and agreement of the CIP Department, or where designated the competent authority:

Provided further that if the CIP Department, or where designated the competent authority, is not responsible for the sector, sub-sector, or type of entity under the First or Second Schedule, the CIP Department shall cooperate with and coordinate measures arising from this sub-article with the designated competent authority in Malta;

(c) upon receipt of a substantiated request from another competent authority, the CIP Department, or where designated the competent authority, shall provide the other competent authority mutual assistance proportionate to its own resources so that the supervisory and enforcement measures may be implemented in an effective, efficient and consistent manner.

(2) The mutual assistance referred to in sub-article (1)(c) may cover information requests and supervisory measures, including requests to carry out on-site inspections or off-site supervision or targeted security audits.

(3) The CIP Department, or where designated the competent authority, shall not refuse the request under sub-article (2), unless it is established that:

(a) it does not have the competence to provide the requested assistance;

(b) the requested assistance is not proportionate to the supervisory tasks of the competent authority; or

(c) the request concerns information or entails activities which, if disclosed or carried out, would be contrary to the essential interests of Malta's national security, public security or defence:

Provided that before refusing such a request, the CIP Department, or where designated the competent authority, shall consult the other competent authorities concerned and upon the request of one of the Member States concerned, the European Commission and ENISA:

Provided further that the notification of such a request to the competent authority of the other Member State shall be done by the CIP Department, or where designated the competent authority.

(4) Where appropriate and with common agreement, the CIP Department, or where designated the competent authority, may carry out joint supervisory actions with competent authorities of various Member States:

Provided that in joint supervisory actions, the CIP Department, or where designated the competent authority may, where appropriate, confer powers, including supervisory and, or enforcement measures under articles 29 and 30 onto the members or staff of the other competent authorities:

Provided further that the joint supervisory actions shall be coordinated by the CIP Department.

PART VIII – ADMINISTRATIVE REVIEW TRIBUNAL

Administrative Review Tribunal.

41. (1) The Administrative Review Tribunal shall be competent to hear and determine appeals from enforcement measures of the CIP Department, or where designated the competent authority, as provided in this order:

Provided that the imposition of administrative penalties pursuant to sub-articles 29(7) and 30(7) shall not be considered as enforcement measures and therefore shall not be subject to appeal before the Administrative Review Tribunal.

Cap. 490.

(2) The provisions of the Administrative Justice Act, in so far as they apply to the Administrative Review Tribunal, shall apply to any proceedings before the said Tribunal and the words 'public administration' in the said enactment shall be construed as a reference to the CIP Department, or where designated the competent authority.

Appeals from enforcement measures.

42. (1) Any essential or important entity shall have a right to appeal to the Administrative Review Tribunal from enforcement measures taken by the CIP Department, or where designated the competent authority which is addressed to it:

Provided that, except for the supervisory measures in sub-articles 29(4) and 30(4), all other supervisory measures are not subject to any appeal.

(2) An appeal from any decision taken by the CIP Department, or where designated the competent authority, shall be made by means of an application and shall be filed with the Secretary of the Administrative Review Tribunal within twenty (20) days from the date on which the said decision has been notified under sub-article 31(5).

(3) In determining an appeal, the Administrative Review Tribunal shall take into account the merits of the appeal, and may in whole or in part, confirm or annul the decision appealed from, giving the reasons for its decisions in writing and shall cause such decision to be made public and communicated to the parties to the appeal.

Right of further appeal.

43. Any party to the proceedings before the Administrative Review Tribunal who feels aggrieved by the said decision, may appeal to the Court of Appeal in its superior competence on a point of law within twenty (20) days from the date of the appealed decision.

RFIRST SCHEDULE
Sectors of High Criticality

Sector	Subsector	Type of entity
1. Energy	(a) Electricity	- Electricity undertakings as defined in Article 2(57) of Directive (EU) 2019/944 of the European Parliament and of the Council ([1]), which carry out the function of 'supply' as defined in Article 2(12) of the said Directive

		- Distribution system operators as defined in Article 2(29) of Directive (EU) 2019/944 - Transmission system operators as defined in Article 2(35) of Directive (EU) 2019/944 - Producers as defined in Article 2(38) of Directive (EU) 2019/944 - Nominated electricity market operators as defined in Article 2(8) of Regulation (EU) 2019/943 of the European Parliament and of the Council (2) - Market participants as defined in Article 2(25) of Regulation (EU) 2019/943 providing aggregation, demand response or energy storage services as defined in Article 2(18), (20) and (59) of Directive (EU) 2019/944 - Operators of a recharging point that are responsible for the management and operation of a recharging point, which provides a recharging service to end users, including in the name and on behalf of a mobility service provider
(b)	District heating and cooling	- Operators of district heating or district cooling as defined in Article 2(19) of Directive (EU) 2018/2001 of the European Parliament and of the Council(3)
(c)	Oil	- Operators of oil transmission pipelines

				- Operators of oil production, refining and treatment facilities, storage and transmission
				- Central stockholding entities as defined in Article 2(f) of Council Directive 2009/119/EC ([4])
		(d)	Gas	- Supply undertakings as defined in Article 2(8) of Directive 2009/73/EC of the European Parliament and of the Council ([5])
				- Distribution system operators as defined in Article 2(6) of Directive 2009/73/EC
				- Transmission system operators as defined in Article 2(4) of Directive 2009/73/EC
				- Storage system operators as defined in Article 2(10) of Directive 2009/73/EC
				- LNG system operators as defined in Article 2(12) of Directive 2009/73/EC
				- Natural gas undertakings as defined in Article 2(1) of Directive 2009/73/EC
				- Operators of natural gas refining and treatment facilities
		(e)	Hydrogen	- Operators of hydrogen production, storage and transmission
2.	Transport	(a)	Air	- Air carriers as defined in Article 3(4) of Regulation (EC) No 300/2008 used for commercial purposes
				- Airport managing bodies as defined in Article 2(2) of Directive 2009/12/EC of the European Parliament and of the Council ([6]), airports as defined in Article 2(1) of the said Directive, including the core airports listed in Section 2 of Annex II to Regulation (EU) No 1315/2013 of the European Parliament and of the Council ([7]), and entities operating ancillary installations contained within airports

		- Traffic management control operators providing air traffic control (ATC) services as defined in Article 2(1) of Regulation (EC) No 549/2004 of the European Parliament and of the Council ([8])
(b)	Rail	- Infrastructure managers as defined in Article 3(2) of Directive 2012/34/EU of the European Parliament and of the Council ([9])
		- Railway undertakings as defined in Article 3(1) of Directive 2012/34/EU, including operators of service facilities as defined in Article 3(12) of the said Directive
(c)	Water	- Inland, sea and coastal passenger and freight water transport companies, as defined for maritime transport in Annex I to Regulation (EC) No 725/2004 of the European Parliament and of the Council ([10]), not including the individual vessels operated by those companies
		- Managing bodies of ports as defined in Article 3(1) of Directive 2005/65/EC of the European Parliament and of the Council ([11]), including their port facilities as defined in Article 2(11) of Regulation (EC) No 725/2004, and entities operating works and equipment contained within ports
		- Operators of vessel traffic services (VTS) as defined in Article 3(o) of Directive 2002/59/EC of the European Parliament and of the Council ([12])
(d)	Road	- Road authorities as defined in Article 2(12) of Commission Delegated Regulation (EU) 2015/962 ([13]) responsible for traffic management control, excluding public entities for which traffic management or the operation of intelligent transport systems is a non-essential part of their general activity

		- Operators of Intelligent Transport Systems as defined in Article 4(1) of Directive 2010/40/EU of the European Parliament and of the Council ([14])
3.	Banking	- Credit institutions as defined in Article 4(1) of Regulation (EU) No 575/2013 of the European Parliament and of the Council (15)
4.	Financial market infrastructures	- Operators of trading venues as defined in Article 4(24) of Directive 2014/65/EU of the European Parliament and of the Council ([16])
		- Central counterparties (CCPs) as defined in Article 2(1) of Regulation (EU) No 648/2012 of the European Parliament and of the Council ([17])
5.	Health	- Healthcare providers as defined in Article 3(g) of Directive 2011/24/EU of the European Parliament and of the Council ([18])
		- EU reference laboratories referred to in Article 15 of Regulation (EU) 2022/2371 of the European Parliament and of the Council ([19])

		- Entities carrying out research and development activities of medicinal products as defined in Article 1(2) of Directive 2001/83/EC of the European Parliament and of the Council ([20])
		- Entities manufacturing basic pharmaceutical products and pharmaceutical preparations referred to in section C division 21 of NACE Rev. 2
		- Entities manufacturing medical devices considered to be critical during a public health emergency (public health emergency critical devices list) within the meaning of Article 22 of Regulation (EU) 2022/123 of the European Parliament and of the Council ([21]))
6.	Drinking water	- Suppliers and distributors of water intended for human consumption as defined in Article 2(1)(a) of Directive (EU) 2020/2184 of the European Parliament and of the Council ([22]), excluding distributors for which distribution of water for human consumption is a non-essential part of their general activity of distributing other commodities and goods
7.	Waste water	- Undertakings collecting, disposing of or treating urban waste water, domestic waste water or industrial waste water as defined in Article 2(1), (2) and (3) of Council Directive 91/271/ EEC ([23]), excluding undertakings for which collecting, disposing of or treating urban waste water, domestic waste water or industrial waste water is a non-essential part of their general activity
8.	Digital infrastructure	- Internet Exchange Point providers - DNS service providers, excluding operators of root name servers

		- TLD name registries - Cloud computing service providers - Data centre service providers - Content delivery network providers - Trust service providers - Providers of public electronic communications networks - Providers of publicly available electronic communications services
9.	ICT service management (business-to-business)	- Managed security providers - Managed security service providers
10.	Public administration	- Public administration entities of central governments as defined by a Member State in accordance with national law - Public administration entities at regional level as defined by a Member State in accordance with national law
11.	Space	- Operators of ground-based infrastructure, owned, managed and operated by Member States or by private parties, that support the provision of space-based services, excluding providers of public electronic communications networks

([1]) Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU (recast) (OJ L 158, 14.6.2019, p. 125).

([2]) Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity (recast) (OJ L 158, 14.6.2019, p. 54).

([3]) Directive (EU) 2018/2001 of the European Parliament and of the Council of 11 December 2018 on the promotion of the use of energy from renewable sources (recast) (OJ L 328, 21.12.2018, p. 82).

([4]) Council Directive 2009/119/EC of 14 September 2009 imposing an obligation on Member States to maintain minimum stocks of crude oil and/or petroleum products (OJ L 265, 9.10.2009, p. 9).

([5]) Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC (OJ L 211, 14.8.2009, p. 94).

(6) Directive 2009/12/EC of the European Parliament and of the Council of 11 March 2009 on airport charges (OJ L 70, 14.3.2009, p. 11).

(7) Regulation (EU) No 1315/2013 of the European Parliament and of the Council of 11 December 2013 on Union guidelines for the development of the trans-European transport network and repealing Decision No 661/2010/EU (OJ L 348, 20.12.2013, p. 1).

(8) Regulation (EC) No 549/2004 of the European Parliament and of the Council of 10 March 2004 laying down the framework for the creation of the single European sky (the framework Regulation) (OJ L 96, 31.3.2004, p. 1).

(9) Directive 2012/34/EU of the European Parliament and of the Council of 21 November 2012 establishing a single European railway area (recast) (OJ L 343, 14.12.2012, p. 32).

(10) Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security (OJ L 129, 29.4.2004, p. 6).

(11) Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security (OJ L 310, 25.11.2005, p. 28).

(12) Directive 2002/59/EC of the European Parliament and of the Council of 27 June 2002 establishing a Community vessel traffic monitoring and information system and repealing Council Directive 93/75/EEC (OJ L 208, 5.8.2002, p. 10).

(13) Commission Delegated Regulation (EU) 2015/962 of 18 December 2014 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU-wide real-time traffic information services (OJ L 157, 23.6.2015, p. 21).

(14) Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport (OJ L 207, 6.8.2010, p. 1).

(15) Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (OJ L 176, 27.6.2013, p. 1).

(16) Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (recast) (OJ L 173, 12.6.2014, p. 349).

(17) Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories (OJ L 201, 27.7.2012, p. 1).

(18) Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4.4.2011, p. 45).

(19) Regulation (EU) 2022/2371 of the European Parliament and of the Council of 23 November 2022 on serious cross-border threats to health and repealing Decision No 1082/2013/EU (OJ L 314, 6.12.2022, p. 26).

(20) Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community code relating to medicinal products for human use (OJ L 311, 28.11.2001, p. 67).

(21) Regulation (EU) 2022/123 of the European Parliament and of the Council of 25 January 2022 on a reinforced role for the European Medicines Agency in crisis preparedness and management for medicinal products and medical devices (OJ L 20, 31.1.2022, p. 1).

(22) Directive (EU) 2020/2184 of the European Parliament and of the Council of 16 December 2020 on the quality of water intended for human consumption (recast) (OJ L 435, 23.12.2020, p. 1).

(23) Council Directive 91/271 of 21 May 1991 concerning urban waste water treatment (OJ L 135, 30.5.1991, p. 40).

SECOND SCHEDULE
Other Critical Sectors

Sector	Subsector	Type of entity
1. Postal and courier services		Postal service providers as defined in Article 2(1a) of Directive 97/67/EC, including providers of courier services
2. Waste management		Undertakings carrying out waste management as defined in Article 3(9) of Directive 2008/98/EC of the European Parliament and of the Council (1), excluding undertakings for whom waste management is not their principal economic activity
3. Manufacture, production and distribution of chemicals		Undertakings carrying out the manufacture of substances and the distribution of substances or mixtures, as referred to in Article 3(9) and (14) of Regulation (EC) No 1907/2006 of the European Parliament and of the Council (2) and undertakings carrying out the production of articles, as defined in Article 3(3) of the said Regulation, from substances or mixtures

4. Production, processing and distribution of food			Food businesses as defined in Article 3(2) of Regulation (EC) No 178/2002 of the European Parliament and of the Council (3) which are engaged in wholesale distribution and industrial production and processing
5. Manufacturing	(a) Manufacture of medical devices and *in vitro* diagnostic medical devices		Entities manufacturing medical devices as defined in Article 2(1) of Regulation (EU) 2017/745 of the European Parliament and of the Council (4), and entities manufacturing *in vitro* diagnostic medical devices as defined in Article 2(2) of Regulation (EU) 2017/746 of the European Parliament and of the Council (5) with the exception of entities manufacturing medical devices referred to in Annex I, point 5, fifth indent, of the said Directive
	(b) Manufacture of computer, electronic and optical products		Undertakings carrying out any of the economic activities referred to in section C division 26 of NACE Rev. 2
	(c) Manufacture of electrical equipment		Undertakings carrying out any of the economic activities referred to in section C division 27 of NACE Rev. 2
	(d) Manufacture of machinery and equipment n.e.c.		Undertakings carrying out any of the economic activities referred to in section C division 28 of NACE Rev. 2
	(e) Manufacture of motor vehicles, trailers and semi-trailers		Undertakings carrying out any of the economic activities referred to in section C division 29 of NACE Rev. 2
	(f) Manufacture of other transport equipment		Undertakings carrying out any of the economic activities referred to in section C division 30 of NACE Rev. 2
6. Digital providers			- Providers of online marketplaces - Providers of online search engines

		- Providers of social networking services platforms
7.	Research	Research organisations

([1]) Directive 2008/98/EC of the European Parliament and of the Council of 19 November 2008 on waste and repealing certain Directives (OJ L 312, 22.11.2008, p. 3).

([2]) Regulation (EC) No 1907/2006 of the European Parliament and of the Council of 18 December 2006 concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH), establishing a European Chemicals Agency, amending Directive 1999/45/EC and repealing Council Regulation (EEC) No 793/93 and Commission Regulation (EC) No 1488/94 as well as Council Directive 76/769/EEC and Commission Directives 91/155/EEC, 93/67/EEC, 93/105/EC and 2000/21/EC (OJ L 396, 30.12.2006, p. 1).

([3]) Regulation (EC) No 178/2002 of the European Parliament and of the Council of 28 January 2002 laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety (OJ L 31, 1.2.2002, p. 1).

([4]) Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (OJ L 117, 5.5.2017, p. 1).

([5]) Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on *in vitro* diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (OJ L 117, 5.5.2017, p. 176).