L.N. 5 of 2026

EUROPEAN UNION ACT
(CAP. 460)

Resilience of Critical Entities and Infrastructures (Identification, Designation and Protection) Order, 2026

IN EXERCISE of the powers conferred by article 3(2) of the European Union Act, the Minister responsible for resilience of critical entities and infrastructures has made the following order:-

PART I
GENERAL PROVISIONS

Citation, scope, commencement and applicability.

1. (1) The title of this order is the Resilience of Critical Entities and Infrastructures (Identification, Designation and Protection) Order, 2026.

(2) The scope of this order is to transpose 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. This order:

(a) establishes national obligations to take specific measures aimed at ensuring that services which are essential for the maintenance of vital societal functions or economic activities within the scope of Article 114 of Treaty on the Functioning of the European Union (TFEU) are provided in an unobstructed manner in the internal market, in particular obligations to identify critical entities and to support critical entities in meeting the obligations imposed on them;

(b) establishes obligations for critical entities aimed at enhancing their resilience and ability to provide services as referred to in paragraph (a) in the internal market;

(c) establishes rules:

(i) on the supervision of critical entities;

(ii) on enforcement;

(iii) for the identification of critical entities of particular European significance and on advisory missions to assess the measures that such entities have established to

satisfy their obligations under Part III;

(d) establishes common procedures for cooperation and reporting on the application of this order;

(e) establishes measures with a view to achieving a high level of resilience of critical entities in order to ensure the provision of essential services within the Union and to improve the functioning of the internal market.

(3) This order shall come into force on such a date as the Minister responsible for the resilience of critical entities and infrastructures may by notice in the Gazette establish, and different dates may be so established for different provisions or different purposes of this order.

S.L. 460.41.

(4) Without prejudice to article 9, this order shall not apply to matters covered by the Measures for a High Common Level of Cybersecurity across the European Union (Malta) Order. In light of the relationship between the physical security and cybersecurity of critical entities, the CIP Department and the designated competent authorities shall ensure that this order and the Measures for a High Common Level of Cybersecurity across the European Union (Malta) Order are being implemented in a coordinated manner.

(5) Where the provisions of sector-specific Union legal acts require critical entities to take measures to enhance their resilience and where those requirements are recognised by the CIP Department and the designated competent authorities as at least equivalent to the corresponding obligations established in this order, the relevant provisions of this order, including the provisions on supervision and enforcement established in Part VI shall not apply.

(6) Without prejudice to Article 346 TFEU, information that is confidential pursuant to Union or national rules, such as rules on business confidentiality, shall be exchanged with the 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 safeguard the confidentiality of such information and the security and commercial interests of critical entities, while respecting the national security.

(7) This order is without prejudice to the national responsibility for safeguarding national security and defence and their power to safeguard other essential State functions, including ensuring

the territorial integrity of the State and maintaining law and order.

(8) This order does 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 investigation, detection and prosecution of criminal offences, nor does it affect the competence of any public administration entity terms in safeguarding other essential national functions, in particular concerning public security, territorial integrity and the maintenance of law and order.

(9) Critical entities which carry out activities in the areas of national security, public security, defence or law enforcement, including the investigation, detection and prosecution of criminal offences, or which provide services exclusively to the public administration entities referred to in sub-article (4) may be exempted from article 10 and Parts III, IV and V, by means of instructions issued by the CIP Department.

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

(11) This order is without prejudice to Union law on the protection of personal data, in particular 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) and the Processing of Personal Data (Electronic Communications Sector) Regulations. S.L. 586.01.

2. In this order, unless the context otherwise requires: Interpretation.

"CIP Department" means the Critical Infrastructure Protection Department as established in accordance with article 3;

"Committee" means the Critical Entities Resilience Committee established by virtue of article 4;

"Commission" means the European Commission;

"competent authorities" means any authority as may from time to time be designated for this purpose in accordance with article 3(2);

"critical entity" means a public or private entity which has been identified by a competent authority in accordance with article 7 as belonging to one of the categories established in the

Schedule;

"critical infrastructure" means an asset, a facility, equipment, a network or a system, or a part of an asset, a facility, equipment, a network or a system, which is necessary for the provision of an essential service;

"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 on the resilience of critical entities and repealing Council Directive 2008/114/EC;

"Director General" means the Director General within the Ministry responsible for the CIP Department;

"essential service" means a service which is crucial for the maintenance of vital societal functions, economic activities, public health and safety, or the environment;

"incident" means an event which has the potential to significantly disrupt, or that disrupts, the provision of an essential service, including when it affects the national systems that safeguard the rule of law;

"Minister" means the Minister responsible for the resilience of critical entities and infrastructures;

"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 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 authorities or by other central-level bodies governed by

public law, 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 authorities or by other central level bodies governed by public law;

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

"Regulation (EU) No 1025/2012" means 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;

"Regulation (EU) 2016/679" means 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);

"Regulation (EU) 2022/2554" means 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;

"resilience" means a critical entity's ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from an incident;

"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 for determining the nature and extent of a risk by identifying and analysing potential relevant threats, vulnerabilities and hazards

which may lead to an incident and by evaluating the potential loss or disruption of the provision of an essential service caused by such incident;

"standard" means a standard as defined in Article 2, paragraph (1) of Regulation (EU) No 1025/2012;

"technical specification" means a technical specification as defined in Article 2, paragraph (4) of Regulation (EU) No 1025/ 2012;

"TFEU" means the Treaty on the Functioning of the European Union;

Cap. 490.

"Tribunal" means the Administrative Review Tribunal established in accordance with the Administrative Justice Act;

"Union" means the European Union.

PART II
NATIONAL FRAMEWORKS ON THE RESILIENCE OF CRITICAL ENTITIES

Competent authorities and the single point of contact.

3. (1) The CIP Department, shall be the national supervisory authority responsible for the monitoring and the application of this order at national level and ensuring compliance therewith, implementing relevant provisions of this order and covering the sectors, sub-sectors and categories of entities found in the Schedule.

(2) The CIP Department shall be designated as the single point of contact to exercise a liaison function for the purpose of ensuring cross-border cooperation with the single points of contact of other Member States and the Critical Entities Resilience Group established in Article 19 of Directive (EU) 2022/2557. The CIP Department shall also act as the single point of contact to exercise a liaison function with the Commission and ensure cooperation with third countries.

(3) With regard to the critical entities in the sectors established in items 3 and 4 of the Schedule, the competent authorities shall in principle, be the competent authorities referred to in Article 46 of Regulation (EU) 2022/2554. With regard to the critical entities in the sector established in the Schedule, the competent authorities shall in principle, be the competent authorities under the Measures for a High Common Level of Cybersecurity across the European Union (Malta) Order.

S.L. 460.41.

(4) The Schedule designates the competent authorities for each

sectors or sub-sectors and clearly establishes the tasks of each competent authorities concerned. The designated competent authorities shall cooperate effectively, under the supervision of the CIP Department as the national supervisory authority, to fulfil their tasks in accordance with this order. The designated competent authorities shall make available to the CIP Department all information and documents required for the CIP Department to ensure compliance with this order.

(5) The CIP Department shall submit, every two (2) years, a summary report to the Commission and to the Critical Entities Resilience Group, on the notifications it has received, including the number of notifications, the nature of notified incidents and the actions taken in accordance with article 22(3).

(6) The CIP Department, or the designated competent authorities, shall have the powers and the adequate financial, human and technical resources to carry out, in an effective and efficient manner, the tasks assigned to them.

(7) The CIP Department and the competent authorities referred to in the Schedule shall, whenever appropriate, consult and cooperate with other relevant national authorities, including the Police, the Armed Forces of Malta, the Information and Data Protection Commissioner, the Department of Civil Protection, and with critical entities and relevant interested parties.

(8) The designated competent authorities listed in the Schedule shall cooperate and exchange information with designated competent authorities under article 8 of the Measures for a High Common Level of Cybersecurity across the European Union (Malta) Order on cybersecurity risks, cyber threats and cyber incidents and non-cyber risks, threats and incidents affecting critical entities, including with regard to relevant measures its designated competent authorities and designated competent authorities under article 7 of the Measures for a High Common Level of Cybersecurity across the European Union (Malta) Order have taken. S.L. 460.41.

(9) Within three (3) months of the designation or establishment of the competent authorities in accordance with this article, their identity, tasks, responsibilities, contact details, and any subsequent changes in that regard shall be communicated to the Commission in accordance with this order.

4. (1) There shall be a Committee designated as the Critical Entities Resilience Committee composed of such members as shall be appointed by the Minister from amongst public officers occupying a senior position and performing duties in the ministries responsible for Critical Entities Resilience Committee.

matters relating to resilience of critical entities and infrastructure as well as from amongst employees occupying a senior position in the other organisations having a main concern in the management, running and control of critical entities and infrastructure in Malta:

Provided that the Minister may appoint other persons as members of the committee who he deems to have the experience and to have shown the capacity in matters relating to resilience of critical entities:

Provided further that the competent authorities listed in the Schedule, other than the CIP Department, may appoint one (1) person as their representative in the Committee.

(2) The Director General responsible for the CIP Department shall be the chairman of the Committee, the Director of this Department shall be the deputy chairman, and one (1) other representative from this Department shall act as the secretary of the Committee. The chairman, deputy chairman and secretary shall not possess voting rights. The deputy chairman shall act instead of the chairman whenever the chairman is absent from a meeting of the Committee or is unable to act as chairman for any reason.

(3) The appointed members shall hold office for such term, that shall not be for more than three (3) years, as may be specified in their letter of appointment.

(4) If any vacancy in the committee 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 Committee and the members thereof may act notwithstanding any such vacancy.

(5) 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 duly performing his functions.

(6) It shall be the duty of the Committee in general to consider and advise the Government, the CIP Department and the designated competent authorities on all matters related to the resilience of critial entities and infrastructure, and in particular:

(a) to advise with regard to the development, maintenance and promotion of an efficient and effective system

of resilience at critical entities and infrastructure to ensure the proper implementation of this order;

(b) to advise with regard to the development and determination of the necessary strategies and policies to reach such objectives; and

(c) the Committee shall issue decisions and give its advice to the CIP Department in relation to the imposition of administrative penalties in accordance with article 24.

(7) The Committee shall meet as often as necessary and shall regulate its own procedures.

(8) The Committee shall decide on the composition and terms of reference of sub-committees or expert groups to which it may delegate special tasks.

(9) With the aim of enhancing the resilience of critical entities identified by the designated competent authorities, and in order to reduce the administrative burden on those critical entities, the Committee shall ensure that this order is applied in a consistent manner. Any designated competent authorities may request the Committee to study the possibility of ensuring a convergent approach regarding interlinked critical entities that use critical infrastructure within Malta, which is physically connected with other Member States, or that belong to the same groups or corporate structures, or that have been identified in Malta and that provide essential services to, or in other Member States.

Strategy on the resilience of critical entities.

5. (1) The CIP Department in cooperation with the competent authorities referred to in the Schedule, shall adopt a national strategy for enhancing the resilience of critical entities hereinafter referred to as the "strategy", The strategy shall be adopted following a consultation, to the extent practically possible, open to relevant stakeholders and shall set out strategic objectives and policy measures, building upon relevant existing national and sectoral strategies, plans or similar documents, with a view to achieving and maintaining a high level of resilience on the part of critical entities and covering at least the sectors set out in the Schedule.

(2) The strategy shall contain at least the following elements:

(a) strategic objectives and priorities for the purposes of enhancing the overall resilience of critical entities, taking into account cross-border and cross-sectoral dependencies and interdependencies;

(b) a governance framework to achieve the strategic objectives and priorities, including a description of the roles and responsibilities of the different authorities, critical entities and other parties involved in the implementation of the strategy;

(c) a description of measures necessary to enhance the overall resilience of critical entities, including a description of the risk assessment referred to in article 6;

(d) a description of the process by which critical entities are identified;

(e) a description of the process supporting critical entities in accordance with this order, including measures to enhance cooperation between the public sector and the private sector and public and private entities;

(f) a list of the main authorities and relevant stakeholders, other than critical entities, involved in the implementation of the strategy;

(g) a policy framework for coordination between the CIP Department and the designated competent authorities in accordance with this order and the designated competent authorities in accordance with article 7 of the Measures for a High Common Level of Cybersecurity across The European Union (Malta) Order for the purposes of information sharing on cybersecurity risks, cyber threats and cyber incidents and non-cyber risks, threats and incidents and the exercise of supervisory tasks;

S.L. 460.41.

(h) a description of measures already in place which aim to facilitate the implementation of obligations in accordance with Part III by small and medium-sized enterprises within the meaning of the Annex to Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises and by small mid-cap enterprises within the meaning of the Annex to Commission Recommendation of 21st May 2025 on the definition of small mid-cap enterprises (2025) 3500 that the Member State in question has identified as critical entities.

(3) Following a consultation that is, to the extent practically possible, open to relevant stakeholders, the CIP Department and the competent authorities listed in the Schedule shall update the strategy at least every four (4) years.

(4) The CIP Department shall communicate the strategy, and

substantial updates thereto to the Commission within three (3) months of their adoption.

(5) The strategy, and substantial updates thereto, shall be approved by the Cabinet before the CIP Department communicates the strategy to the Commission and before the strategy may be implemented by the CIP Department and the designated competent authorities.

National Risk Assessment.

6. (1) The CIP Department, in cooperation with the competent authorities, shall ensure that National Risk Assessments are conducted utilising the list of essential services established and potentially updated by the Commission from time to time. The CIP Department or, the competent authorities shall utilise the National Risk Assessments to identify critical entities in accordance with article 7. The CIP Department or, the competent authorities shall use the National Risk Assessment to assist those critical entities in taking measures pursuant to article 13. The National Risk Assessments shall be updated whenever necessary and at least every four (4) years:

Provided that the risk assessments shall account for the relevant natural and man-made risks, including those of a cross-sectoral or cross-border nature, accidents, natural disasters, public health emergencies and hybrid threats or other antagonistic threats, including terrorist offences as provided for under Sub-title IV A of Title IX of Part II of Book First the Criminal Code.

Cap. 9.

(2) The National Risk Assessments shall take into account at least the following:

(a) the general risk assessment carried out pursuant to Article 6(1) of Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism;

(b) other relevant risk assessments, carried out in accordance with the requirements of the relevant sector-specific Union legal acts, including Regulation (EU) 2017/1938 of the European Parliament and of the Council of 25 October 2017 concerning measures to safeguard the security of gas supply and repealing Regulation (EU) No 994/2010 and (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC and the Assessment and Management of Flood Risks Regulations and the Control of Major Accident Hazards Regulations;

S.L. 549.167.
S.L. 646.12.

(c) the relevant risks arising from the extent to which the

sectors established in the Schedule depend on one another, including the extent to which they depend on entities located within other Member States and in third countries, and the impact that a significant disruption in one (1) sector may have on other sectors, including any significant risks to citizens and the internal market:

Provided that for the purposes of this paragraph, the CIP Department or, the competent authorities shall cooperate with the competent authorities of other Member States and the competent authorities of third countries, as appropriate.

(d) any information on incidents notified in accordance with article 18.

(3) The competent authorities shall carry out the relevant elements of the risk assessments referred to in this article available to the critical entities that are identified in accordance with article 7. The competent authorities shall obtain approval from the CIP Department before disseminating the relevant elements of the risk assessments. The CIP Department and the competent authorities shall ensure that the information provided to critical entities assists them in carrying out their risk assessments pursuant to article 12 and in taking measures to ensure their resilience pursuant to article 13.

(4) Within three (3) months of carrying out the National Risk Assessment referred to in this article, the CIP Department shall provide the Commission with relevant information on the types of risks identified and the outcomes of, following such risk assessment referred to in this article, per sector and sub-sector as established in the Schedule.

Identification of critical entities.

7. (1) The competent authorities shall identify the critical entities in the sectors and sub-sectors established in the Schedule, that fall under their responsibility.

(2) When the competent authorities identify critical entities pursuant to sub-article (1), they shall take into account the outcomes of the risk assessments and the strategy referred to in articles 5 and 6 and shall apply the following criteria:

(a) the entity provides one (1) or more essential services;

(b) the entity operates and its critical infrastructure is located on the territory of Malta; and

(c) an incident would have significant disruptive effects,

as determined in accordance with sub-article (1) of article 8, on the provision by the entity of one (1) or more essential services or on the provision of other essential services in the sectors established in the Schedule that depend on that or those essential services.

(3) The competent authorities shall establish a list of the critical entities identified pursuant to sub-articles (1) and (2) and ensure that those critical entities are notified that they have been identified as critical entities within one (1) month of such identification. When notifying the critical entities, the designated competent authorities shall also notify the CIP Department. This Department shall maintain a national list of critical entities identified by the competent authorities:

Provided that the designated competent authorities shall inform those critical entities of their obligations under Parts III, IV and V and the date from which those obligations apply to them, without prejudice to article 8. The CIP Department or the designated competent authorities of this order shall inform critical entities in the sectors established in the Schedule that they have no obligations under Parts III, IV, and V unless national measures provide otherwise. When notifying the critical entities, the designed competent authorities shall also notify the CIP Department:

Provided further that for the critical entities concerned, Part III shall apply after ten (10) months from the date of the notification referred to in the first paragraph of this article.

(4) The CIP Department or the designated competent authorities shall notify the competent authorities designated in accordance with article 7 of the Measures for a High Common Level of Cybersecurity across the European Union (Malta) Order of the identity of the critical entities that they have identified in accordance with this article within one (1) month of such identification. Such notification shall specify, where applicable, that the critical entities concerned are entities in the sectors established in the Schedule and have no obligations in accordance with Parts III, IV and V. When notifying the designated competent authorities in accordance with the Measures for a High Common Level of Cybersecurity across the European Union (Malta) Order, of the identity of the critical entities, the designated competent authorities shall also notify the CIP Department. S.L. 460.41.

(5) The competent authorities shall, where necessary and in any event at least every four (4) years review and where appropriate, update the list of identified critical entities referred to in sub-article

(3). Where those updates lead to the identification of additional critical entities, sub-articles (3) and (4) shall apply to those additional critical entities. In addition, they shall ensure that entities that are no longer identified as critical entities following any such update are notified in due time of the fact that they are no longer subject to the obligations under Parts III, IV and V from the date of receipt of such notification. When notifying additional critical entities or when notifying critical entities that are no longer identified as critical entities, the competent authorities shall also notify the CIP Department that shall update the national list of critical entities.

Significant disruptive effect.

8. (1) When determining the significance of a disruptive effect as referred to in paragraph (c) of sub-article (2) of article 7 the competent authorities shall take into account the following criteria:

(a) the number of users relying on the essential service provided by the entity concerned;

(b) the extent to which other sectors and sub-sectors as established in the Schedule depend on the essential service in question;

(c) the impact that incidents may have, in terms of degree and duration, on economic and societal activities, the environment, public safety and security, or the health of the population;

(d) the entity's market share in the market for the essential service or essential services concerned;

(e) the geographic area that may be affected by an incident, including any cross-border impact, taking into account the vulnerability associated with the degree of isolation of certain types of geographic areas, such as insular regions or remote regions;

(f) the importance of the entity in maintaining a sufficient level of the essential service, taking into account the availability of alternative means for the provision of such essential service.

(2) After the identification of the critical entities in accordance with sub-article (1) of article 7, the competent authorities shall submit the following information to the Commission without undue delay:

(a) a list of essential services within Malta where there are any additional essential services as compared to the list of essential services referred to in sub-article (1) in article 7;

(b) the number of critical entities identified for each sector and sub-sector established in the Schedule for each essential service;

(c) any thresholds applied to specify one (1) or more of the criteria in sub-article (1). Thresholds may be presented as such or in aggregated form.

(3) The CIP Department shall subsequently submit information referred to in sub-article (2) whenever necessary and at least every four (4) years.

Critical entities in the banking, financial market infrastructure and digital infrastructure sectors.

9. The CIP Department and designated competent authorities shall ensure that article 13 and Parts III, IV and V do not apply to critical entities that are identified in the sectors established in the Schedule where these critical entities are already subject to at least equivalent measures by virtue of other national law:

Provided that the CIP Department or the designated competent authorities may make recommendations to the Minister to adopt or maintain provisions of national law that achieve a higher level of resilience for those critical entities, provided that these recommendations are in accordance with applicable Union law.

Support to critical entities.

10. (1) The CIP Department and designated competent authorities shall support critical entities in enhancing their resilience. Such support may include developing guidance materials and methodologies, supporting the organisation of exercises to test their resilience and providing advice and training to the personnel of critical entities. Without prejudice to applicable rules on State aid, the CIP Department or the designated competent authorities may recommend financial resources to critical entities, where necessary and justified by public interest objectives and national circumstances:

Provided that the CIP Department or the designated competent authorities may make recommendations to the Prime Minister for the support of financial resources to critical entities, in consultation with the Minister and the Minister responsible for the sector, sub-sector or type of entity in the Schedule. The financial support shall be without prejudice to the application of competition rules established in the TFEU:

Provided further that the designated competent authorities shall also notify the CIP Department when support to critical entities is provided.

(2) The CIP Department and the designated competent authorities shall cooperate and exchange information and good

practices with critical entities of the sectors established in the Schedule.

(3) The CIP Department and the designated competent authorities of this order shall facilitate voluntary information sharing between critical entities in relation to matters covered by this order, in accordance with Union law on classified and sensitive information, competition and protection of personal data and national law including but not limited to the Official Secrets Act, the Competition Act and the Data Protection Act.

Cap. 50.
Cap. 379.
Cap. 586.

(4) Where necessary and justified by public interest objectives, the CIP Department or the designated competent authorities shall facilitate voluntary information sharing and the exchange of good practices between critical entities.

Cooperation between Member States.

11. (1) Whenever appropriate, the CIP Department and the designated competent authorities shall consult other competent authorities in other Member States regarding critical entities for the purpose of ensuring that this order is applied in a consistent manner. When notifying competent authorities in other Member States, the designated competent authorities in Malta shall also notify the CIP Department. Such consultations shall take place regarding critical entities that:

(a) use critical infrastructure which is physically connected between two (2) or more Member States;

(b) are part of corporate structures that relate to, or are linked to critical entities in other Member States;

(c) have been identified as critical entities in one (1) Member State and provide essential services to, or in other Member States.

(2) The consultations referred to in sub-article (1) shall aim at enhancing the resilience of critical entities and, where possible, reducing the administrative burden on them.

PART III
RESILIENCE OF CRITICAL ENTITIES

Risk assessment by critical entities.

12. (1) Notwithstanding the deadline established in article 7(3), the CIP Department, or the designated competent authorities shall ensure that critical entities carry out a risk assessment within nine (9) months of receiving the notification referred to in article 7(3), whenever necessary subsequently, and at least every four (4) years, on the basis of the national risk assessment and other relevant sources of

information, in order to assess all relevant risks that could disrupt the provision of their essential services (critical entity risk assessment).

(2) Critical entity risk assessments shall account for all the relevant natural and human-caused risks which may lead to an incident, including those of a cross-sectoral or cross-border nature, accidents, natural disasters, public health emergencies and hybrid threats and other antagonistic threats, including terrorist offences as provided for under Sub-title IV A of Title IX of Part II of Book First of the Criminal Code. A critical entity risk assessment shall take into account the extent to which other sectors as established in the Schedule depend on the essential service provided by the critical entity and the extent to which such critical entity depends on essential services provided by other entities in such other sectors, including where relevant in Member States and third countries: Cap. 9.

Provided that where a critical entity has carried out other risk assessments or drawn up documents pursuant to obligations established in other legal acts that are relevant for its critical entity risk assessment, it may use those assessments and documents to satisfy the requirements established in this article:

Provided further that when exercising its supervisory functions, the competent authorities may declare an existing risk assessment carried out by a critical entity that addresses the risks and extent of dependence referred to in the first proviso conforms, in whole or in part, with the obligations in accordance with this article.

Resilience measures of critical entities.

13. (1) The CIP Department, or the designated competent authorities, shall ensure that critical entities take appropriate and proportionate technical, security and organisational measures to ensure their resilience, based on the relevant information provided by Malta on the National Risk Assessment and on the outcomes of the critical entity risk assessment, including measures necessary to:

(a) prevent incidents from occurring, duly considering disaster risk reduction and climate adaptation measures;

(b) ensure adequate physical protection of their premises and critical infrastructure, duly considering, for example, fencing, barriers, perimeter monitoring tools and routines, detection equipment and access controls;

(c) respond to, resist, and mitigate the consequences of incidents, duly considering the implementation of risk and crisis management procedures and protocols and alert routines;

(d) recover from incidents, duly considering business

continuity measures and the identification of alternative supply chains, to ensure the continuity of the provision of the essential service;

(e) ensure adequate employee security management, duly considering measures including establishing categories of personnel who exercise critical functions, establishing access rights to premises, critical infrastructure and sensitive information, the establishment of procedures for background checks in accordance with article 15 and designating the categories of persons who are required to undergo such background checks, and establishing appropriate training requirements and qualifications:

Provided that for the purposes of this paragraph, the CIP Department, or designated competent authorities shall ensure that critical entities consider the personnel of external service providers when establishing categories of personnel who exercise critical functions.

(f) raise awareness about the measures referred to in paragraphs (a) to (e) among relevant personnel, duly considering training courses, information materials and exercises:

(2) Critical entities shall develop and keep updated a resilience plan or equivalent documents which describe the measures taken pursuant to sub-article (1). The plan or equivalent documents shall include internal quality control measures describing how compliance with the plan is to be monitored by the critical entities. The plan or equivalent documents shall be submitted to the designated competent authorities, which may either approve it or direct the critical entity to make any necessary amendments. Once approved by the designated competent authorities, the entities shall ensure that all measures described in the plan are fully implemented. A copy of the plan with the approval letter from the designated competent authorities shall be submitted to the CIP Department by the critical entities:

Provided that where critical entities have drawn up documents or taken measures pursuant to obligations established in other legal acts that are relevant for the measures referred to in sub-article (1), they may use those documents and measures to satisfy the requirements established in this article. When exercising its supervisory functions, the competent authorities may declare existing resilience-enhancing measures taken by a critical entity that address, in an appropriate and proportionate manner, the technical, security and organisational measures referred to in sub-article (1) as compliant, in whole or in part, with the obligations under this article.

(3) Critical entities shall designate at least one (1) security liaison officer (SLO) or the equivalent and inform the CIP Department and the designated competent authorities. The security liaison officer (SLO) or the equivalent shall act as the point of contact with the CIP Department and the designated competent authorities. The security liaison officer shall ensure that the measures described in the resilience plan or equivalent documents are fully implemented. The security liaison officer shall ensure that internal quality control activities are conducted so to ensure compliance with the resilience plan or equivalent documents.

Advisory mission.

14. (1) The CIP Department, or the designated competent authorities that has identified the critical entity, with the agreement of the critical entity concerned, may request the Commission to organise advisory missions, in accordance with the arrangements established in this order, to provide advice to the critical entity concerned in meeting its obligations in accordance with this Part III. The advisory mission shall report its findings to the Commission and the critical entity concerned.

(2) The CIP Department or the designated competent authorities that has identified a critical entity of particular European significance as a critical entity pursuant to article 20(1), may request the Commission to organise an advisory mission and they shall have access to the measures that such critical entity has put in place to satifsy its obligations in accordance with this Part:

Provided that in cases where the essential service is offered within Malta, the CIP Department or, the designated competent authorities, with the agreement of the Member State where the critical entity has been identified as a critical entity of a particular European significance pursuant to article 20(1), may request the Commission to organise an advisory mission, as referred to in sub-article (5):

Provided further that the CIP Department or the designated competent authorities, which has identified a critical entity of particular European significance as a critical entity pursuant to article 20(1), shall upon a reasoned request from the Commission or one (1) or more Member States, provide the following:

(a) the relevant parts of the critical entity risk assessment;

(b) a list of relevant measures taken in accordance with article 13;

(c) supervisory or enforcement actions, including

assessments of compliance or orders issued, that its competent authorities have undertaken pursuant to Part V of this order in respect of such critical entity:

Provided that in cases where the essential service is offered within Malta, the CIP Department and the designated competent authorities shall analyse the report with the findings submitted by the advisory mission and, where necessary, shall advise the Commission on whether the critical entity of particular European significance concerned complies with its obligations in accordance with this Part and, where appropriate, on the measures that may be taken to improve the resilience of such critical entity:

Provided further that the CIP Department or the designated competent authorities that has identified a critical entity of particular European significance as a critical entity pursuant to article 20(1), shall ensure that the critical entity concerned takes into account the Commission's opinion on the report referred to in the sub-article (1) and provides information to the Commission and the Member States to, or in which the essential service is provided on the measures it has taken pursuant to that opinion.

(3) When the essential service is offered within Malta or the critical entity of particular European significance is located within Malta, the CIP Department or the designated competent authorities may propose candidates to be part of an advisory mission:

Provided that whenever necessary, members of the advisory mission shall have valid and appropriate security clearance. The Commission shall bear the costs related to participation in advisory missions.

(4) The CIP Department or the designated competent authorities shall ensure that critical entities of particular European significance provide advisory missions with access to information, systems and facilities relating to the provision of their essential services necessary for carrying out the advisory mission concerned.

(5) Advisory missions carried out in Malta shall comply with applicable national law and with respect to the responsibility for national security and the protection of national security interests, including but not limited to the Official Secrets Act, the Competition Act and the Data Protection Act.

Cap. 50.
Cap. 379.
Cap. 586.

Background checks.

15. (1) Critical entities shall conduct backgrounds checks on persons who:

(a) hold sensitive roles in, or for the benefit of the critical entity, in particular in relation to the resilience of the critical entity;

(b) are authorised to directly or remotely access its premises, information or control systems, including in connection with the security of the critical entity;

(c) are under consideration for recruitment to positions that fall under the criteria established in paragraph (a) or (b).

(2) To conduct background checks on persons, the management bodies of critical entities shall:

(a) establish the person's identity on the basis of documentary evidence;

(b) collect and verify the criminal records of the person in all states of residence during at least the preceding five (5) years. A "state of residence" shall be any country in which the person has been resident continuously for at least six (6) months:

Provided that when carrying out background checks, the management bodies of critical entities shall use the European Criminal Records Information System in accordance with the procedures established in Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States and, where relevant and applicable, Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726 for the purpose of obtaining information from criminal records held by other Member States. The central authorities referred to in article 3(1) of Framework Decision 2009/315/JHA and in article 3(5) of Regulation (EU) 2019/816, shall provide replies to requests for such information within ten (10) working days from the date on which the request was received in accordance with article 8(1) of Framework Decision 2009/315/JHA.

(3) The management bodies of critical entities shall not allow a person to hold the roles and positions referred to in sub-article (1) if from the information indicated in the criminal records it results that the person has been found guilty of an offence and the punishment awarded was of a term of imprisonment of thirty (30) months or more,

whether or otherwise such term of imprisonment has been suspended.

(4) Requests as referred to in this article shall be assessed within a reasonable timeframe and processed in accordance with the Data Protection Act and relevant and applicable Union law. Background checks shall be proportionate and strictly limited to what is necessary. They shall be carried out for the sole purpose of evaluating a potential security risk to the critical entity concerned.

Cap. 586.

Rehabilitation periods.

16. (1) If from the information indicated in the criminal records it results that the person has been found guilty of an offence and the punishment awarded was of a term of imprisonment of a period between eighteen (18) months and thirty (30) months, whether or otherwise such term of imprisonment has been suspended, the person may hold the roles and positions referred to in article 15(1) after the lapse of ten (10) years from the date of the final judgement regarding such conviction.

(2) If from the information indicated in the criminal records it results that the person has been found guilty of an offence and the punishment awarded was of a term of imprisonment of a period between seven (7) months and seventeen (17) months, whether or otherwise such term of imprisonment has been suspended, the person may hold the roles and positions referred to in article 15(1) after the lapse of eight (8) years from the date of the final judgement regarding such conviction.

(3) If from the information indicated in the criminal records it results that the person has been found guilty of an offence and the punishment awarded was of a term of imprisonment of six (6) months or less, whether or otherwise such term of imprisonment has been suspended, the person may hold the roles and positions referred to in article 15(1) after the lapse of seven (7) years from the date of the final judgement regarding such conviction.

(4) The periods of rehabilitation referred to in sub-articles (1) and (3) shall be halved in the case of persons who were below the age of eighteen (18) years, on the date of the commission of the offence.

(5) If from the information indicated in the criminal records, it results that the person has been found guilty of an offence but the punishment prescribed did not include a term of imprisonment, then the person shall be allowed to hold the roles and positions referred to in article 15(1).

(6) If from the information indicated in the criminal records, it results that the person has been charged with the commission of an offence but was acquitted, then the person shall be allowed to hold the

roles and positions referred to in article 15(1).

Recurrent background checks.

17. (1) The management bodies of critical entities shall collect from persons already holding roles and positions referred to in article 15(1), criminal records at specific intervals not exceeding two (2) years.

(2) If from the information indicated in criminal records, it results that a person already holding the roles and positions referred to in article 15(1) has been found guilty of an offence and the punishment awarded was of a term of imprisonment, whether or otherwise such term of imprisonment has been suspended, then the person shall be removed from the roles and positions referred to in article 15(1):

Provided that the person shall be allowed to hold the roles and positions referred to in article 16(1) once the appropriate rehabilitation periods in article 15 have elapsed.

Incident notification.

18. (1) The CIP Department or the designated competent authorities shall ensure that the critical entities notify the competent authorities, without undue delay, of incidents that significantly disrupt or have the potential to significantly disrupt the provision of essential services. The CIP Department or the designated competent authorities shall ensure that, unless operationally unable to do so, critical entities submit an initial notification not later than twenty-four (24) hours after becoming aware of an incident, followed where relevant, by a detailed report not later than one (1) month thereafter. To determine the significance of a disruption, the following parameters shall be considered:

(a) the number and proportion of users affected by the disruption;

(b) the duration of the disruption;

(c) the geographical area affected by the disruption, considering whether the area is geographically isolated;

(d) the sectors affected by the disruption of the essential service;

(e) the dependency of a critical entity, essential entities, important entity on the disruption of the essential services:

Provided that the management bodies of critical entities shall submit to the CIP Department and the designated competent authorities, a more detailed report within seventy-two (72) hours after becoming aware of such incident. Such report shall include the current

mitigation measures that the critical entities are implementing. Within one (1) month from the incident the critical entities shall provide a final report of the incident that includes the suspected root cause of the incident:

Provided further that where an incident has or might have a significant impact on the continuity of the provision of essential services to or in six (6) or more Member States, the CIP Department shall notify the Commission of such incident.

(2) Notifications referred to in sub-article (1) shall include any available information necessary to enable the designated competent authorities to understand the nature, cause, and consequences of the incident, including any available information necessary to determine any cross-border impact of the incident. Such notifications shall not subject critical entities to increased liability.

(3) On the basis of the information provided by a critical entity by means of a notification referred to in sub-article (1), the CIP Department, shall inform the single point of contact of other affected Member States where the incident has, or might have a significant impact on critical entities and the continuity of the provision of essential services to, or in one or more other Member States:

Provided that the CIP Department in sending and receiving information in accordance with sub-article (1) shall, in conformity with Union Law or with the Official Secrets Act, treat that information in a way that respects its confidentiality and protects the security and commercial interest of the critical entity concerned.

Cap. 50.

(4) As soon as possible following a notification in accordance with sub-article (1), the competent authorities concerned shall provide the critical entity concerned with relevant follow-up information, including information that may support such critical entity's effective response to the incident in question. The CIP Department or the designated competent authorities shall inform the public where they determine that it is in the public interest to do so.

(5) When addressing incidents resulting in personal data breaches, the CIP Department, or the designated competent authorities, shall work in close cooperation with the Information and Data Protection Commissioner, in accordance with the Data Protection Act and relevant subsidiary legislation, without prejudice to the competence and tasks of the Commissioner under the said legislation.

Cap. 586.

Standardisation.

19. In order to promote the convergent implementation of this order, the CIP Department or the designated competent authorities, shall where useful, and 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 and resilience measures applicable to critical entities.

PART IV
CRITICAL ENTITIES OF PARTICULAR EUROPEAN SIGNIFICANCE

Identification of critical entities of European significance.

20. (1) An entity shall be considered a critical entity of European significance where it:

(a) has been identified as a critical entity in accordance with article 7(1);

(b) provides the same or similar essential services to, or in six (6) or more Member States; and

(c) has been notified in accordance with sub-article (3).

(2) Critical entities, following the notification in accordance with article 7(3), shall inform the CIP Department, or the designated competent authority, when it provides essential services to, or in six (6) or more Member States. In such cases, the CIP Department, or the designated competent authorities shall ensure that the critical entity informs them of the essential services it provides to, or in those Member States, as well as the Member States to which, or in which it provides such essential services. The designated competent authorities shall inform the CIP Department of the list of identified critical entities of European significance. The CIP Department shall notify the Commission, without undue delay, of the identity of such critical entities and of the information they provide in accordance with this sub-article:

Provided that during the consultation carried out by the Commission, the CIP Department shall inform the Commission where it deems that the services provided in Malta by the critical entity are essential services.

(3) Where the Commission notifies the CIP Department or the designated competent authorities, that an entity was designated as a critical entity of particular European significance, the CIP Department, or the designated competent authorities, shall forward such notification to the designated critical entity without undue delay, whilst informing it of its obligations in accordance with this order and the date from which those obligations apply to it.

(4) This Part shall apply to the designated critical entity of European significance concerned from the date of receipt of the notification referred to in sub-article (3).

PART V
SUPERVISION AND ENFORCEMENT

General aspects concerning supervision and enforcement.

21. (1) In order to assess the compliance of the entities identified as critical entities pursuant with the obligations established in this order, the CIP Department or the designated competent authorities shall have the powers and means to:

(a) conduct on-site inspections of the critical infrastructure and the premises that the critical entity uses to provide its essential services and off-site supervision of measures taken by critical entities in accordance with article 13 of this order;

(b) conduct or order audits in respect of critical entities.

(2) The CIP Department and the competent authorities shall have the powers and means to require, critical entities to provide within a reasonable time limit established by the CIP Department or the competent authorities:

(a) the information necessary to assess whether the measures taken by those entities to ensure their resilience satisfy the requirements established in article 13 of this order;

(b) evidence of the effective implementation of those measures, including the results of internal quality control activities. Internal quality control activities may include an audit conducted by an independent and qualified auditor selected by the respective critical entity and conducted at its expense;

(c) access to other data, documents and information necessary for the CIP Department, or the designated competent authorities, to carry out their supervisory tasks;

(d) a resilience plan or equivalent documents:

Provided that when requiring such information, the CIP Department or the competent authorities shall state the purpose of the requirement and specify the information required.

(3) Without prejudice to the possibility to impose administrative penalties, the CIP Department or the competent authorities may, following the supervisory actions referred to in sub-

article (1) or the assessment of the information referred to in sub-article (2), order the critical entities concerned to take the necessary and proportionate measures to remedy any identified breach of this order, within a reasonable time limit established by those authorities and to provide those authorities with information on the measures taken. Those orders shall take into account, in particular, the seriousness of the breaches.

(4) The CIP Department or the competent authorities shall ensure that the powers provided for in this article may only be exercised subject to appropriate safeguards. Those safeguards shall guarantee, in particular, that such exercise takes place in an objective, transparent and proportionate manner and that the rights and legitimate interests of the critical entities affected, such as the protection of trade and business secrets, are duly safeguarded, including the right to be heard, the right of defence and the right to an effective remedy before an independent court.

(5) The CIP Department or the competent authorities shall, when assessing the compliance of a critical entity pursuant to this article, inform the competent authorities of the Member States concerned under Measures for a High Common Level of Cybersecurity across the European Union (Malta) Order. The CIP Department or the competent authorities shall ensure that competent authorities in accordance with this order, may request the competent authorities under the Measures for a High Common Level of Cybersecurity across the European Union (Malta) Order, to exercise their supervisory and enforcement powers in relation to an entity under that order that has been identified as a critical entity under this order. The CIP Department or the competent authorities shall cooperate and exchange information with the competent authorities under the Measures for a High Common Level of Cybersecurity across the European Union (Malta) Order. S.L. 460.41.

Breach of personal data.

22. (1) When the CIP Department or the designated competent authorities become aware in the course of supervision or enforcement that the breach by a critical entity of the obligations established in this order may entail a personal data breach, as defined in Article 4(12) of Regulation (EU) 2016/679, it shall without undue delay, inform the Information and Data Protection Commissioner in accordance with Articles 33, 55 and 56 of Regulation (EU) 2016/679.

(2) When the Information and Data Protection Commissioner imposes an administrative fine in accordance with Part VI of the Data Protection Act, the CIP Department, or the designated competent authorities, shall not impose an administrative penalty in accordance with article 24 for a breach in accordance with sub-article (1) arising Cap. 586.

from the same conduct as that which was the subject of the administrative fine under Part VI of the said Act. The CIP Department, or the designated competent authorities may however, impose the enforcement measures provided for in article 24.

(3) When the supervisory competent authority is not established in Malta in accordance with Regulation (EU) 2016/679, the CIP Department or the designated competent authorities, shall inform the Information and Data Protection Commissioner of the potential data breach referred to in sub-article (1).

Supervisory measures in relation to critical entities.

23. (1) The CIP Department or the competent authorities shall ensure that critical entities establish, update and implement a resilience plan or equivalent documents. The approved resilience plan or equivalent documents shall be monitored and regularly audited by the CIP Department or the competent authorities.

(2) The CIP Department or the competent authorities shall, after carrying out an audit or other compliance monitoring activity on a critical entity, draw up a report stating the findings.

(3) The CIP Department or the competent authorities shall classify these findings into one of the following four (4) categories:

(a) fully compliant;

(b) compliant but improvement desired;

(c) not compliant; or

(d) not compliant with serious breaches.

(4) The CIP Department or the competent authorities shall give reasons for the decision to classify the findings as such. The report shall be communicated to the critical entity. Failure by critical entities to submit a resilience plan or equivalent documents for approval by the designated competent authorities shall be classified by the CIP Department or the competent authorities as being "not compliant with serious breaches".

(5) If the findings are classified by the CIP Department or the competent authorities as being "not complaint" or "not compliant with serious breaches" the critical entity shall, within two (2) weeks from receipt of the report, submit an action plan wherein there shall be indicated the corrective actions which are to be taken by the critical entity to address the breaches, including the deadlines when such breaches shall be fully rectified.

(6) The CIP Department or the competent authorities shall examine the action plan and may either approve it or direct the critical entity concerned to make the necessary amendments within a stipulated period of time. The implementation of the action plan shall be monitored by the CIP Department or the competent authorities.

(7) If a critical entity fails to submit an action plan, fails to amend the action plan as necessary or fails to comply with the approved action plan, the CIP Department or the competent authorities may, depending on the severity and the particular circumstances of the case:

(a) give advice or make recommendations to the critical entity in order to explain the need to rectify the breaches identified during the compliance monitoring activities;

(b) issue a formal warning whereby the critical entity is directed to immediately rectify its breaches; and, or

(c) report the breaches to the Committee:

Provided that the CIP Department or the competent authorities shall inform the critical entity that failure to rectify its breaches may lead to the imposition of administrative penalties in accordance with this order.

Enforcement measures in relation to critical entities.

24. (1) The Critical Entities Resilience Committee shall have the power to impose administrative penalties on any critical entity reported by the CIP Department or the competent authorities, as being non-compliant with the approved resilience plan or equivalent documents.

(2) Prior to deciding on whether critical entities, are compliant with the approved resilience plan or equivalent documents or otherwise, the Committee shall allow the critical entity concerned to provide documentation or make submissions as it deems fit.

(3) The Committee may, if it deems necessary, request more information or documentation from the CIP Department or the competent authorities or from the critical entity concerned.

(4) The Committee shall give reasons for its decision.

(5) Whenever the Committee finds that a critical entity has not complied with the approved resilience plan or equivalent documents and has not taken the necessary measures to remedy the breaches, it shall impose an administrative penalty. If the findings are classified by the CIP Department or the competent authorities as being "not

complaint" the administrative penalty shall be of two thousand five hundred euro (€2,500). If the findings are classified by the CIP Department or the competent authorities as being "not compliant with serious breaches" the administrative penalty shall be of five thousand euro (€5,000).

(6) In its decision, the Committee shall provide a time-frame within which the critical entity, shall pay the administrative penalty and a time-frame within which the critical entity is to remedy its breaches:

Provided that if the critical entity does not pay the administrative penalty and, or does not remedy its breaches within the stipulated time-frame, the Committee shall impose a further administrative penalty equal to the administrative penalty originally imposed and, or a penalty of one hundred euro (€100) for each day during which the deficiency subsists. Any daily penalty imposed, may be backdated to the date of the commission or commencement of the breach.

Administrative Review Tribunal.

25. (1) Any decision taken by the Committee in accordance with this order may be contested within twenty (20) days from service of the decision by means of an application filed before the Administrative Review Tribunal.

(2) Any party to an appeal who feels aggrieved by a decision of the Administrative Review Tribunal may, on a point of law, appeal from such decision by filing an application to the Court of Appeal constituted in accordance with article 41(9) of the Code of Organization and Civil Procedure. Such application shall be filed within twenty (20) days from the date of the decision of the Administrative Review Tribunal.

Cap. 12.

Cap. 12.

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

Repeal and saving. S.L. 460.24.

26. The Critical Infrastructures and European Critical Infrastructures (Identification, Designation and Protection) Order are hereby being repealed:

Provided that any act, decision or action, however so described, taken before the coming into force of this order shall remain to be regulated by the provisions of the Critical Infrastructures and European Critical Infrastructures (Identification, Designation and Protection) Order as in force prior to the coming into force of this order.

S.L. 460.24.

27. In the Second Schedule to the Administrative Justice Act, immediately after the last item of the subsidiary legislation there shall be added the following new item: Consequential amendment. Cap. 490.

"Resilience of Critical Entities and Infrastructures (Identification, Designation and Protection) Order, 2025, S.L. 460.43, Inferior Competence".

SCHEDULE

SECTORS, SUBSECTORS AND CATEGORIES OF ENTITIES
(article 3)

SCHEDULE

SECTORS, SUBSECTORS AND CATEGORIES OF ENTITIES
(article 3)

Sectors Subsectors Categories of entities	**Sectors Subsectors Categories of entities**	**Sectors Subsectors Categories of entities**	**Competent authorities**
1. Energy	(a) Electricity	Electricity undertakings as defined in Article 2, point (57), of Directive (EU) 2019/944 of the European Parliament and of the Council, which carry out the function of "supply" as defined in Article 2, point (12), of that Directive	CIP Department as the national supervisory authority.
		Distribution system operators as defined in Article 2, point (29), of Directive (EU) 2019/944	
		Transmission system operators as defined in Article 2, point (35), of Directive (EU) 2019/944	
		Producers as defined in Article 2, point (38), of Directive (EU) 2019/944	
		Nominated electricity market operators as defined in Article 2, point (8), of Regulation (EU) 2019/943 of the European Parliament and of the Council	
		Market participants as defined in Article 2, point (25), of Regulation (EU) 2019/943 providing aggregation, demand response or energy storage	

		services as defined in Article 2, points (18), (20) and (59), of Directive (EU) 2019/944	
	(b) District heating and cooling	Operators of district heating or district cooling as defined in Article 2, point (19), of Directive (EU) 2018/2001 of the European Parliament and of the Council	CIP Department as the national supervisory authority.
	(c) Oil	Operators of oil transmission pipelines	CIP Department as the national supervisory authority.
		Operators of oil production, refining and treatment facilities, storage and transmission	
		Central stockholding entities as defined in Article 2, point (f), of Council Directive 2009/119/EC	
	(d) Gas	Supply undertakings as defined in Article 2, point (8), of Directive 2009/73/EC of the European Parliament and of the Council	CIP Department as the national supervisory authority.
		Distribution system operators as defined in Article 2, point (6), of Directive 2009/73/EC	
		Transmission system operators as defined in Article 2, point (4), of Directive 2009/73/EC	
		Storage system operators as defined in Article 2,point (10), of Directive 2009/73/EC	
		LNG system operators as defined in Article 2, point (12), of Directive 2009/73/EC	

		Natural gas undertakings as defined in Article 2, point (1), of Directive 2009/73/EC	
		Operators of natural gas refining and treatment facilities	
	(e) Hydrogen	Operators of hydrogen production, storage and	CIP Department as the national supervisory authority.
2. Transport	(a) Air	Air carriers as defined in Article 3, point (4), of Regulation (EC) No 300/2008 used for commercial purposes	CIP Department as the national supervisory authority.
		Airport managing bodies as defined in Article 2, point (2), of Directive 2009/12/EC of the European Parliament and of the Council, airports as defined in Article 2, point (1), of that Directive, including the core airports listed in Section 2 of Annex II to Regulation (EU) 2024/1679 of the European Parliament and of the Council of 13 June 2024 on Union guidelines for the development of the trans-European transport network, amending Regulations (EU) 2021/1153 and (EU) No 913/2010 and repealing Regulation (EU) No 1315/2013, and entities operating ancillary installations contained within airports	

		Traffic management control operators providing air traffic control (ATC) services as defined in Article 2, point (1), of Regulation (EC) No 549/2004 of the European Parliament and of the Council	
	(b) Rail	Infrastructure managers as defined in Article 3, point (2), of Directive 2012/34/EU of the European Parliament and of the Council	Not applicable
		Railway undertakings as defined in Article 3, point (1), of Directive 2012/34/EU and operators of service facilities as defined in Article 3, point (12), of that Directive	Not applicable
	(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, not including the individual vessels operated by those companies	CIP Department as the national supervisory authority.
		Managing bodies of ports as defined in Article 3, point (1), of Directive 2005/65/EC, including their port facilities as defined in Article 2, point (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, point (o), of Directive 2002/59/EC of the European Parliament and of the Council	
	(d) Road	Road authorities as defined in Article 2, point (12), of Commission Delegated Regulation (EU) 2015/962 responsible for traffic management control, excluding public entities for whom traffic-management or the operation of intelligent transport systems is a non-essential part of their general activity	CIP Department as the national supervisory authority.
		Operators of Intelligent Transport Systems as defined in Article 4, point (1), of Directive 2010/40/EU of the European Parliament and of the Council	
	(e) Public Transport	Public service operators as defined in Article 2, point (d), of Regulation (EC) No 1370/2007 of the European Parliament and of the Council	CIP Department as the national supervisory authority.
3. Banking sector		Credit institutions as defined in Article 4, point (1), of Regulation (EU) No 575/2013	CIP Department as the national supervisory authority.
4. Financial Market Infrastructure		Operators of trading venues as defined in Article 4, point (24), of Directive 2014/65/EU	CIP Department as the national supervisory authority.
		Central counterparties (CCPs) as defined in Article	

		2, point (1), of Regulation (EU) No 648/2012	
5. Health		Healthcare providers as defined in Article 3, point (g), of Directive 2011/24/EU of the European Parliament and of the Council	CIP Department as the national supervisory authority.
		EU reference laboratories as referred to in Article 15 of Regulation (EU) 2022/2371 of the European Parliament and of the Council	
		Entities carrying out research and development activities of medicinal products as defined in Article 1, point (2), of Directive 2001/83/EC of the European Parliament and of the Council	
		Entities manufacturing basic pharmaceutical products and pharmaceutical preparations as referred to in Section C division 21 of NACE Rev. 2	
		Entities manufacturing medical devices considered as 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	

		Entities holding a distribution authorisation as referred to in Article 79 of Directive 2001/83/EC	
6. Drinking water		Suppliers and distributors of water intended for human consumption as defined in Article 2, point (1)(a), of Directive (EU) 2020/2184 of the European Parliament and of the Council, 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	CIP Department as the national supervisory authority.
7. Waste water		Undertakings collecting, disposing of or treating urban waste water, domestic waste water or industrial waste water as defined in Article 2, points (1), (2) and (3), of Council Directive 91/271/EEC, 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	CIP Department as the national supervisory authority.
8. Digital infrastructure		Providers of internet exchange points	Malta Communications Authority (MCA).
		DNS service providers as excluding operators of root name servers	
		Top-level-domain name registries	

		Providers of cloud computing services	
		Providers of data center services	
		Providers of content delivery networks	
		Trust service providers	
		Providers of electronic communications services	
		Providers of publicly available electronic communications services	
9. Public administration		Public administration entities of central governments and at regional level as defined by Member States in accordance with national law.	CIP Department as the national supervisory authority.
		Public administration entities that provide broadcasting and transmission services deliver essential and emergency services, including public safety alerts, by offering radio broadcasts and emergency announcements in both analogue and digital formats.	
10. 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 as defined in Article 2, point (8), of Directive (EU) 2018/1972	CIP Department as the national supervisory authority.

11. Production, processing and distribution of food		Food businesses as defined in Article 3, point (2), of Regulation (EC) No 178/2002 of the European Parliament and of the Council which are engaged exclusively in logistics and wholesale distribution and large scale industrial production and processing	CIP Department as the national supervisory authority.

VERŻJONI ELETTRONIKA

Ippubblikat mid-Dipartiment tal-Informazzjoni (doi.gov.mt) — Valletta — ***Published by the Department of Information (doi.gov.mt) — Valletta***
Mitbugħ fl-Istamperija tal-Gvern fuq karta FSC — ***Printed at the Government Printing Press on FSC certified paper***

Prezz/*Price*
€3.69