L.N. 89 of 2026

EUROPEAN UNION ACT
(CAP. 460)

Measures for a High Common Level of Cybersecurity across the European Union (Malta) (Amendment) Order, 2026

IN EXERCISE of the powers conferred by article 4(2) of the European Union Act, the Minister responsible for critical infrastructure protection has made the following order:-

Citation.

1. The title of this order is the Measures for a High Common Level of Cybersecurity across the European Union (Malta) (Amendment) Order, 2026 and this order shall be read and construed as one with the Measures for a High Common Level of Cybersecurity across the European Union (Malta) Order, hereinafter referred to as the "principal order". S.L. 460.41.

Amends article 2 of the principal order.

2. Article 2 of the principal order shall be amended as follows:

(a) the definition "Advisory Board" shall be deleted;

(b) immediately after the definition "Commission Recommendation 2003/361/EC" there shall be added the following new definition:

" "Committee" means the Enforcement Committee established by virtue of article 5;";

(c) the definition "CSIRT" shall be substituted by the following new definition:

" "CSIRT" means a computer security incident response team;";

(d) the definition "CSIRTs network" shall be substituted by the following new definition:

" "CSIRTs network" means the network of national CSIRTs established in accordance with Article 15 of the Directive (EU) 2022/2555;";

(e) the definition "Director" shall be substituted by the following new definition:

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

(f) the definition "National Cyber Security Steering Committee" shall be substituted by the following new definition:

" "National Cyber Security Steering Committee" means the Committee as established in accordance with article 15;";

(g) immediately after the definition "National Cyber Security Steering Committee", as substituted, there shall be added the following new definition:

" "national CSIRT" means the national computer security incident response team designated or established in accordance with article 8;".

Amends article 3 of the principal order.

3. Paragraph (b) of sub-article (17) of article 3 of the principal order shall be substituted by the following new paragraph:

" (b) the sector-specific Union legal act provides for immediate access, where appropriate automatic and direct, to the incident notifications by the CSIRTs, the CIP Department or where designated the competent authorities 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).".

Amends title to Part II of the principal order.

4. The title of Part II of the principal order shall be substituted by the following new title:

"**PART II – ENFORCEMENT COMMITTEE, CRITICAL INFRASTRUCTURE PROTECTION DEPARTMENT AND CSIRTs**".

Substitutes article 5 of the principal order.

5. Article 5 of the principal order shall be substituted by the

following new article:

"Enforcement Committee.

5. (1) There shall be a committee designated as the Enforcement 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 matters relating to cybersecurity of essential and important entities, as well as from amongst employees occupying a senior position in the other organisations having a main interest in the management, running and control of cybersecurity at essential or important entities in Malta:

Provided that the Minister may appoint other persons as members of the Committee who appear to him to have the experience and to have shown the capacity in matters relating to cyber resilience of essential and important entities:

Provided further that the competent authorities listed in the First and Second Schedules, 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 chairperson of the Committee, the Director of this Department shall be the deputy chairperson, and one other representative from this Department shall act as the secretary of the Committee. The chairperson, deputy chairperson and secretary shall not possess voting rights. The deputy chairperson shall act instead of the chairperson whenever the chairperson is absent from a meeting of the Committee or is unable to act as chairperson for any reason.

(3) The appointed members shall hold office for such term, that shall not be 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 properly performing his functions.

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

Substitutes article 6 of the principal order.

6. Article 6 of the principal order shall be substituted by the following new article:

"Function of the Committee.

6. It shall be the duty of the Committee to issue decisions in relation to the imposition of an administrative penalty in accordance with articles 32, 33, 34 and 38.".

Substitutes article 7 of the principal order.

7. Article 7 of the principal order shall be substituted by the following new article:

"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 tables to the First and Second Schedules:

Provided that as the national supervisory authority the CIP Department shall be responsible for:

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

(b) building partnerships with operators of critical information infrastructures for information sharing, without prejudice to article 26;

(c) 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);

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

(e) adopting the strategy on the security of network and information systems, as detailed in the National Cybersecurity Strategy in accordance with article 15;

(f) supervising and enforcing measures on all CSIRTs in accordance with articles 29 and 30;

(g) managing an internal cybersecurity operations center and an internal CSIRT;

(h) acting as a coordinator for the purposes of the coordinated vulnerability disclosure in accordance with article 13(1); and

(i) ensuring effective, efficient and secure cooperation in the Cooperation Group.

(2) The First and Second Schedules designate the competent authorities for each sectors or sub-sectors and clearly establish 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 under this order. The designated competent authorities shall make available to the CIP Department all information and documents required for the Department to ensure compliance with this Order.

(3) 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) identifying and designating essential and important entities;

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

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

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

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

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

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

(h) supervising and enforcing measures on essential and important entities, and on all CSIRTs in accordance with articles 29 and 30:

Provided that the CIP Department shall be deemed as duly authorised in the carrying out of any of the above measures in accordance with article 337C(2) of the Criminal Code:

Cap. 9.

Provided further 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 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:

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:

Provided further that the national CSIRT shall have access to the register as defined in article 7(1)(d) as maintained and updated by the CIP Department.

(4) 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 3(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.

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

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

(7) The Director General or his delegate shall represent the CIP Department in any judicial proceedings.".

8. Article 8 of the principal order shall be amended as follows: Amends article 8 of the principal order.

(a) the marginal note thereof shall be substituted by the following new marginal note

"National CSIRT.";

(b) in sub-article (1) thereof the words "CIP Department" shall be substituted by the words "Malta Information Technology Agency";

(c) in sub-article (2) thereof immediately before the words "CSIRT shall:" there shall be added the words "The national";

(d) in sub-article (3) thereof immediately before the words "CSIRT may establish cooperation" there shall be added the words "The national";

(e) in sub-article (4) thereof immediately before the words "CSIRT may:" there shall be added the words "the national".

Substitutes article 10 of the principal order.

9. Article 10 of the principal order shall be substituted by the following new article:

"Tasks of the national CSIRT and of the internal and autonomous CSIRTs.

10. (1) The national 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 as the leading national representative, 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, provided that the CIP Department may participate in the CSIRTs network;

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

(2) The national 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 and 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 the national 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.

Provided further that the national CSIRT shall notify the CIP Department, and where designated, the other competent authorities, about all the assistance, information, scanning, incidence response or other services that are to be provided to the essential and important entities in line with any of the provisions of this article.

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

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

(5) In order to facilitate cooperation referred to in sub-article (4), the national CSIRT shall promote the adoption and use of common or standardised practices, classification schemes and taxonomies in relation to incident-handling procedures.

(6) 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).".

Amends article 11 of the principal order.

10. In article 11 of the principal order the words "to the CIP Department, and CSIRT" shall be substituted by the words "to the CIP Department, to the national CSIRT and to the designated competent authorities".

11. Article 12 of the principal order shall be amended as follows: Amends article 12 of the principal order.

(a) in sub-article (1) thereof immediately after the words "The CIP Department," there shall be added the words "the national";

(b) sub-article (2) thereof shall be substituted by the following new sub-article:

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

(c) in sub-article (3) thereof immediately before the words "CSIRT shall inform" there shall be added the words "The national";

(d) sub-article (4) thereof shall be substituted by the following new sub-article:

"(4) The CIP Department, and where designated, the competent authority, and national CSIRT shall cooperate with the Executive Police, the Office of the Information and Data Protection Commissioner in accordance with the Data Protection Act, the Aviation Security Department 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, the 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.

(e) sub-article (5) thereof shall be substituted by the following new sub-article:

"(5) The CIP Department and the national CSIRT shall exchange relevant information on a regular basis, including with regard to relevant incidents and cyber threats with competent authorities under this order.";

(f) sub-article (8) thereof shall be deleted.

Substitutes article 13 of the principal order.

12. Article 13 of the principal order shall be substituted by the following new article:

"Coordinated vulnerability disclosure.

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

Provided that the CIP Department shall immediately notify in writing to the national CSIRT any vulnerabilities reported to it. The CIP Department shall immediately notify in writing any other designated competent authority or authorities, as the case may be, of any vulnerabilities reported to it that has a significant impact on the provision of the services provided by an essential or important entity which such authority regulates.

(2) The CIP Department 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 the CIP Department designated as coordinator for vulnerability disclosure shall include:

(a) the adoption of common or standardised practices, classification schemes and taxonomies;

(b) identifying and contacting the entities concerned;

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

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

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

(4) Any person shall be able to report, anonymously, a vulnerability to the CIP Department. The CIP Department shall ensure the anonymity and confidentiality of the persons throughout the vulnerability disclosure.

(5) The CIP Department 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, the national 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 accordance with article 337C of the Criminal Code, insofar as the reporting natural or legal person complies with the coordinated vulnerability disclosure policy of such entity.

Cap. 9.

(8) The CIP Department shall carry out the technical operations strictly necessary for the characterisation of the risk or threat referred to in this article:

Provided that the CIP Department 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.

13. Article 14 of the principal order shall be amended as follows:

Amends article 14 of the principal order.

(a) sub-article (4) thereof shall be substituted by the following new sub-article:

"(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) independent from the essential or important entity being audited, including submitting a Declaration of Independence as determined by the CIP Department;

(b) 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;

(c) in possession of a valid European and, or international cybersecurity certification or cybersecurity standard as determined by the CIP Department; and

(d) experienced and has skillsets as determined by the CIP Department.".

Amends article 15 of the principal order.

14. Immediately after sub-article (1) of article 15 of the principal order there shall be added the following new sub-article:

"(1a) The National Cyber Security Steering Committee shall also:

(a) act as the national point of reference on cybersecurity within the public sector, private sector and the public together with the respective sectorial and implementing entities;

(b) provide a coordinated response to cybersecurity incidents upon request of the Chairperson; and

(c) provide guidance on cybersecurity policy and technical matters upon request of Ministries and entities.".

Adds a new article to the principal order.

15. Immediately after article 15 of the principal order there shall be added the following new article:

"National Cyber Security Steering Committee.

15A. (1) The National Cyber Security Steering Committee shall be composed of the following members:

(a) the Principal Permanent Secretary or his delegate;

(b) a representative of the Ministry responsible for foreign affairs;

(c) a representative of the Ministry responsible for home affairs;

(d) a representative of the Malta Information Technology Agency;

(e) a representative of the Malta Financial Services Authority;

(f) a representative of the Malta Gaming Authority;

(g) a representative of the Malta Communications Authority;

(h) a representative of the Malta Digital Innovation Authority;

(i) a representative of the National Security Authority;

(j) a representative of the Malta Police Force;

(k) a representative of the Armed Forces; and

(l) a representative of the CIP Department.

(2) The National Cyber Security Steering Committee may, whenever it deems so necessary or expedient, engage one (1) or more persons, whom it considers to be in possession of suitable expertise and security clearance, to assist it in carrying out specific tasks requiring such expertise.

(3) The National Cyber Security Steering Committee may also establish sub-committees focusing on specific and thematic areas to assist the National Cyber Security Steering Committee. The sub-committees established under the authority of the National Cyber Security Steering Committee shall operate internally and exclusively within the functional remit of the National Cyber Security Steering Committee and shall not possess autonomous decision-making powers unless expressly delegated by the said Committee.

(4) The Chairperson of the National Cyber Security Steering Committee shall be the Principal Permanent Secretary or his delegate.

(5) A Deputy Chairperson shall be appointed by the Principal Permanent Secretary from among the members of the National Cyber Security Steering Committee.

(6) The meetings of the National Cyber Security Steering Committee shall be chaired by the Chairperson or, in the absence of the Chairperson, by the Deputy Chairperson.

(7) The National Cyber Security Steering Committee shall meet at such regular intervals, and shall as a minimum meet once every two (2) months.

(8) The members of the National Cyber Security Steering Committee and experts appointed in accordance with sub-article (1) shall treat any information acquired in the performance of their duties or the exercise of the functions as part of the National Cyber Security Steering Committee as confidential.".

Amends article 16 of the principal order.

16. Article 16 of the principal order shall be amended as follows:

(a) sub-article (2) thereof shall be substituted by the following new sub-article:

"(2) The plan shall establish, in particular:

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

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

(c) the cyber crisis management procedures, including their integration into the general national crisis management framework and information exchange means;

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

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

(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; and

(g) the common or standardised practices, classification schemes and taxonomies to be used in relation to cyber crisis management.";

(b) sub-article (5) thereof shall be substituted by the following new sub-article:

"(5) The CIP Department shall be the leading 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 (EU) 2022/ 2555. The national CSIRT may also participate in the European cyber crisis liaison organisation network.".

17. In article 17 of the principal order immediately after the words "CIP Department in cooperation with" there shall be added the words " the national". Amends article 17 of the principal order.

18. Article 20 of the principal order shall be amended as follows: Amends article 20 of the principal order.

(a) sub-article (1) thereof shall be substituted by the following new sub-article:

"(1) Essential and important entities shall immediately notify the national 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 the national CSIRT shall immediately notify in writing the CIP Department and any other designated competent authority 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.";

(b) in sub-article (2) thereof immediately after the words "any information enabling" there shall be added the words "the national";

(c) sub-article (5) thereof shall be substituted by the following new sub-article:

"(5) For the purpose of notification in accordance with sub-article (1), the entities concerned shall submit to the national 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 the national 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 the national CSIRT with a progress report at that time and a final report within one (1) month of their handling of the incident.";

(d) in sub-article (6) thereof immediately after the words "trust services, notify" there shall be added the words "the national";

(e) sub-article (7) thereof shall be substituted by the following new sub-article:

"(7) The national 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 the national 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 the national CSIRT. The national CSIRT shall provide additional technical support if the entity concerned so requests, provided the technical capability is available.";

(f) sub-article (8) thereof shall be substituted by the following new sub-article:

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

(g) sub-article (9) thereof shall be substituted by the following new sub-article:

"(9) Where appropriate, and in particular where the significant incident concerns Malta and at least another Member State, the national CSIRT, with prior coordination with the CIP Department and where designated the competent authority, 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, the national 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.";

(h) in sub-article (10) thereof immediately after the words "in the public interest," there shall be added the words "the national";

(i) in sub-article (11) thereof immediately after the words "At the request of" there shall be added the words "the national";

(j) in sub-article (12) thereof immediately before the words "CSIRT shall provide" there shall be added the words "The national";

(k) in sub-article (13) thereof immediately after the words "submit to ENISA" there shall be added the words "and to

the National Cybersecurity Steering Committee,".

Amends article 26 of the principal order.

19. Article 26 of the principal order shall be amended as follows:

(a) in sub-article (1) thereof immediately before the words "CSIRT shall ensure" there shall be added the words "The national";

(b) in sub-article (2) thereof immediately before the words "CSIRT shall ensure" there shall be added the words "The national";

(c) sub-article (3) thereof shall be substituted by the following new sub-article:

"(3) The national 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, the national CSIRT may impose conditions on the information made available by any competent authority or CSIRTs. The national CSIRT shall offer assistance for the application of such arrangements in accordance with its policies provided for in article 15(3)(h).".

Amends article 27 of the principal order.

20. Article 27 of the principal order shall be amended as follows:

(a) in sub-article (1) thereof immediately after the words "notifications may be submitted to" there shall be added the words "the national";

(b) in sub-article (2) thereof immediately before the words "CSIRT shall process" there shall be added the words "The national";

(c) in sub-article (3) thereof immediately after the words "Where applicable," there shall be added the words "the national".

Amends article 28 of the principal order.

21. Sub-article (4) of article 28 of the principal order shall be substituted by the following new sub-article:

"(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 under article 31(10)(a) and (b) shall not be applicable to public administration entities subject to this order.".

22. Article 29 of the principal order shall be amended as follows: Amends article 29 of the principal order.

(a) sub-article (4) thereof shall be substituted by the following new sub-article:

"(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.";

(b) sub-article (7) thereof shall be substituted by the following new sub-article:

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

23. Article 30 of the principal order shall be amended as follows: Amends article 30 of the principal order.

(a) sub-article (4) thereof shall be substituted by the following new sub-article:

"(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 essential entity, except in duly substantiated cases when the CIP Department, or where

designated the competent authority shall decide otherwise.";

(b) sub-article (7) thereof shall be substituted by the following new sub-article:

"(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 Committee, in accordance with national law pursuant to article 33.".

Amends article 31 of the principal order.

24. Article 31 of the principal order shall be amended as follows:

(a) sub-articles (6), (7) and (8) thereof shall be deleted;

(b) paragraph (b) of sub-article (10) thereof, with the exception of the provisos, shall be substituted by the following new paragraph:

"(b) request the relevant bodies, courts or tribunals, 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:".

Amends article 32 of the principal order.

25. Article 32 of the principal order shall be amended as follows:

(a) sub-article (2) thereof shall be substituted by the following new sub-article:

"(2) Where the CIP Department, or where designated the competent authority, requests the imposition of an administrative penalty and at the same time, 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).";

(b) sub-article (6) thereof shall be deleted.

Substitutes article 33 of the principal order.

26. Article 33 of the principal order shall be substituted by the

following new article:

"Power of the Enforcement Committee to impose administrative fines.

33. (1) The Enforcement Committee shall have the power to impose administrative fines established by this order, on any entity reported by the CIP Department, or where designated the competent authority, as being non-compliant with this order.

(2) Prior to deciding on whether an entity is compliant with this order, the Committee shall allow the entity to provide documentation or make submissions as it deems fit.

(3) The Committee may, if it deems necessary, ask for more information or documentation from the CIP Department, or where designated the competent authority, or from the entity concerned.

(4) Whenever the Committee establishes that an entity has not complied with this order or has not taken the necessary supervisory or enforcement measures in accordance with this order, it shall impose an administrative fine.

(5) In its decision the Committee shall indicate the amount of the administrative penalty and a timeframe within which the entity concerned shall pay the administrative penalty, as well as a timeframe within which the entity is to remedy the breach. The Committee shall give reasons for its decision.".

Amends article 34 of the principal order.

27. Article 34 of the principal order shall be amended as follows:

(a) paragraph (b) of sub-article (1) thereof shall be substituted by the following new paragraph:

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

(b) sub-article (2) thereof shall be substituted by the following new sub-article:

"(2) The Committee shall notify the entity concerned of the following:

(a) the administrative penalty that shall be imposed;

(b) the specific reasons on the basis of which the administrative penalty shall 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.";

(c) sub-articles (3), (4), (5) and (6) thereof shall be deleted.

Deletes article 35 of the principal order.

28. Article 35 of the principal order shall be deleted.

Deletes article 36 of the principal order.

29. Article 36 of the principal order shall be deleted.

Amends article 37 of the principal order.

30. Sub-article (2) of article 37 of the principal order shall be substituted by the following new sub-article:

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

Substitutes article 38 of the principal order.

31. Article 38 of the principal order shall be substituted by the following new article:

"Daily penalty payments.

38. (1) The CIP Department, or where designated the competent authority, may request the imposition by the Committee of daily 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 penalty payment shall be one hundred euro (€100) for each breach in terms of sub-article (1), for each day during which the breach persists:

Provided that any daily penalty payment imposed may be backdated to the date on which the breach was committed or the breach commenced.

(3) When deciding about daily penalty payments, the Committee shall act in accordance with articles 33 and 34.".

Amends article 39 of the principal order.

32. Sub-article (2) of article 39 of the principal order shall be substituted by the following new sub-article:

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

Substitutes article 41 of the principal order.

33. Article 41 of the principal order shall be substituted by the following new article:

"Administrative Review Tribunal.

41. (1) Any decision taken by the Committee in accordance with this order may be appealed within twenty (20) days from the 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 question 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.

(3) 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.".

Cap. 12.

Deletes article 42 of the principal order.

34. Article 42 of the principal order shall be deleted.

Deletes article 43 of the principal order.

35. Article 43 of the principal order shall be deleted.

Substitutes the First Schedule to the principal order.

36. The First Schedule to the principal order shall be substituted by the following new Schedule:

B 728

FIRST SCHEDULE

Sectors, Subsectors,
Types of Entities of High Criticality and Competent Authorities
(in accordance with article 4)

Sector	Subsectors	Type of entity/entities	Competent authority/ authorities
1. Energy	(a) Electricity	(i) 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 said Directive;	CIP Department as the national supervisory authority.
		(ii) Distribution system operators as defined in Article 2, point (29), of Directive (EU) 2019/944;	
		(iii) Transmission system operators as defined in Article 2, point (35), of Directive (EU) 2019/944;	
		(iv) Producers as defined in Article 2, point (38), of Directive (EU) 2019/944;	
		(v) Nominated electricity market operators as defined in Article 2, point (8), of Regulation (EU) 2019/943 of the European Parliament and of the Council;	
		(vi) 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;	
		(vii) 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	(i) 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	(i) Operators of oil transmission pipelines;	CIP Department as the national supervisory authority.
		(ii) Operators of oil production, refining and treatment facilities, storage and transmission;	
		(iii) Central stockholding entities as defined in Article 2, point (f), of Council Directive 2009/119/EC;	

	(d) Gas	(i) 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.
		(ii) Distribution system operators as defined in Article 2, point (6), of Directive 2009/73/EC;	
		(iii) Transmission system operators as defined in Article 2, point (4), of Directive 2009/73/EC;	
		(iv) Storage system operators as defined in Article 2, point (10), of Directive 2009/73/EC;	
		(v) LNG system operators as defined in Article 2, point (12), of Directive 2009/73/EC;	
		(vi) Natural gas undertakings as defined in Article 2, point (1), of Directive 2009/73/EC;	
		(vii) Operators of natural gas refining and treatment facilities.	
	(e) Hydrogen	(i) Operators of hydrogen production, storage and transmission operators.	CIP Department as the national supervisory authority.

B 730

2. Transport	(a) Air	(i) 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.
		(ii) 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 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, and entities operating ancillary installations contained within airports;	
		(iii) 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	(i) Infrastructure managers as defined in Article 3, point (2), of Directive 2012/34/EU of the European Parliament and of the Council;	Not applicable.
		(ii) 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 said Directive.	
	(c) Water	(i) 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.
		(ii) 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	
		(iii) 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	(i) 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.
		(ii) 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	(i) 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		(i) 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		(i) Operators of trading venues as defined in Article 4, point (24), of Directive 2014/65/EU.	CIP Department as the national supervisory authority.
		(ii) Central counterparties (CCPs) as defined in Article 2, point (1), of Regulation (EU) No 648/2012.	

5. Health		(i) 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.
		(ii) EU reference laboratories as referred to in Article 15 of Regulation (EU) 2022/2371 of the European Parliament and of the Council;	
		(iii) 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;	
		(iv) Entities manufacturing basic pharmaceutical products and pharmaceutical preparations as referred to in Section C division 21 of NACE Rev. 2	
		(v) 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;	
		(vi) Entities holding a distribution authorization as referred to in Article 79 of Directive 2001/83/EC.	
6. Drinking water		(i) 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		(i) 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		(i) Providers of internet exchange points;	Malta Communications Authority (MCA).
		(ii) DNS service providers as excluding operators of root name servers;	
		(iii) Top-level-domain name registries;	
		(iv) Providers of cloud computing services;	
		(v) Providers of data center services;	
		(vi) Providers of content delivery networks;	
		(vii) Trust service providers;	
		(viii)Providers of electronic communications services;	
		(ix) Providers of publicly available electronic communications services.	
9. ICT services management (business-to-business)		(i) Managed service providers;	CIP Department as the national supervisory authority.
		(ii) Managed security service providers.	
10. Public administration		(i) 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.
		(ii) 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.	
11. Space		(i) 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.

(b) The Second Schedule to the principal order shall be substituted by the following new Schedule:

Substitutes the Second Schedule to the principal order.

SECOND SCHEDULE

Other Sectors, Subsectors,
Types of Entities of High Criticality and Competent Authorities
(in accordance with article 4)

Sector	Subsector	Type of entity/entities	Competent authority/ authorities
1. Postal and courier services		(i) Postal service providers as defined in Article 2, point (1a), of Directive 97/67/EC, including providers of courier services.	Malta Communications Authority (MCA).
2. Waste management		(i) Undertakings carrying out waste management as defined in Article 3, point (9), of Directive 2008/98/EC of the European Parliament and of the Council, excluding undertakings for whom waste management is not their principal economic activity.	CIP Department as the national supervisory authority.
3. Manufacture, production and distribution of chemicals		(i) Undertakings carrying out the manufacture of substances and the distribution of substances or mixtures, as referred to in Article 3, points (9) and (14), of Regulation (EC) No 1907/2006 of the European Parliament and of the Council and undertakings carrying out the production of articles, as defined in Article 3, point (3), of said Regulation, from substances or mixtures.	CIP Department as the national supervisory authority.
4. Production, processing and distribution of food		(i) 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 in wholesale distribution and industrial production and processing.	CIP Department as the national supervisory authority.

5. Manufacturing	(a) Manufacture of medical devices and *in vitro* diagnostic medical devices	(i) Entities manufacturing medical devices as defined in Article 2, point (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, point (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 item 5(v) of the First Schedule.	CIP Department as the national supervisory authority.
	(b) Manufacture of computer, electronic and optical products	(i) Undertakings carrying out any of the economic activities referred to in section C division 26 of NACE Rev. 2.	
	(c) Manufacture of electrical equipment	(i) 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.	(i) 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	(i) 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	(i) Undertakings carrying out any of the economic activities referred to in section C division 30 of NACE Rev. 2.	
6. Digital providers		(i) Providers of online marketplaces;	Malta Communications Authority (MCA).
		(ii) Providers of online search engines;	
		(iii) Providers of social networking services platforms.	
7. Research		(i) Research organizations.	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*
€2.97